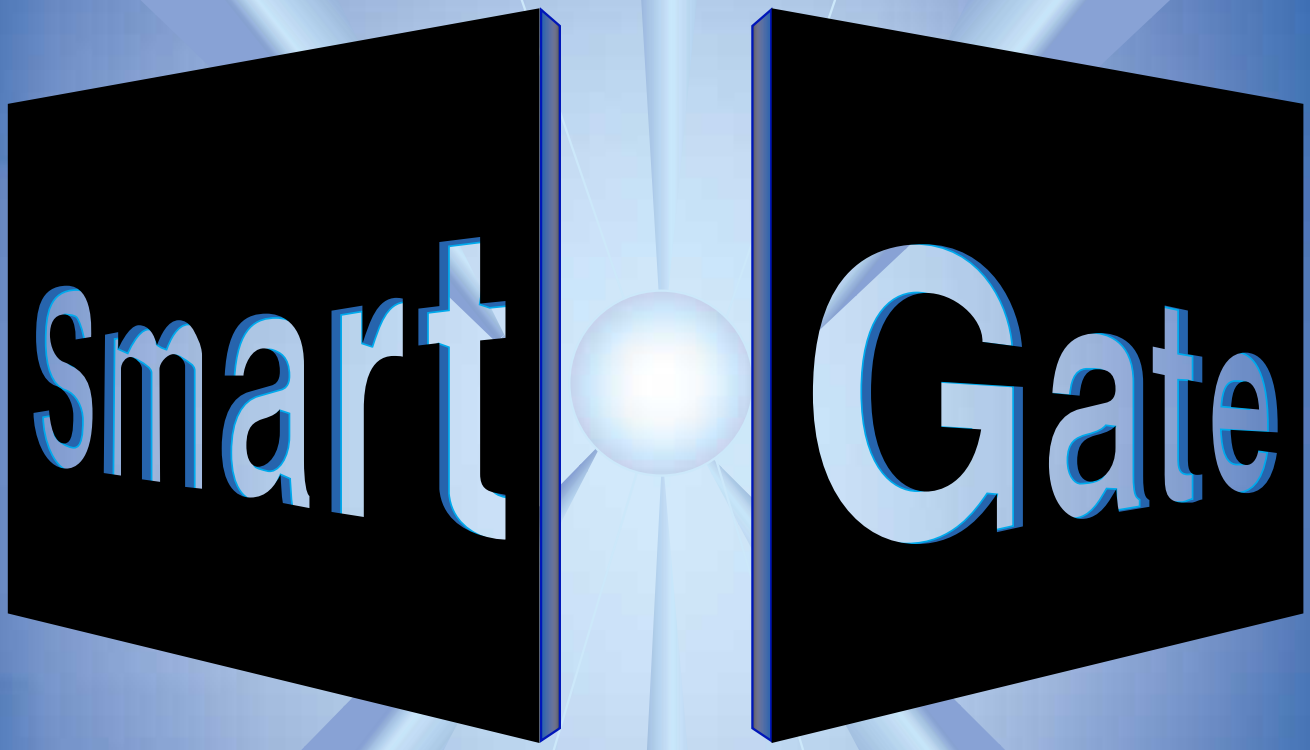
SmartPass®

Administrator's Guide



V-ONE

Security for a Connected World™

Published by
V–ONE Corporation
20250 Century Boulevard, Suite 300
Germantown, Maryland 20874
(301) 515–5200
(800) 495–VONE (8663)
(301) 515–5280 (FAX)

V–ONE Corporation Technical Support
(800) 495–VONE (8663)

(888) 220–VONE (8663)
(24-Hour Support)

(301) 515–5260
(International Support)

Contents

Overview **7**
Purpose of This Guide 7
Organization of This Guide 8
Appendix 8
Sources of Help 8
Typographic Conventions 9

Chapter 1 Introduction to SmartGate **11**
SmartGate System Components 12
SmartGate Server 13
SmartPass Software 13
Authentication Methods 13
Access Code 14
Hardware and Software Requirements for SmartPass 14
PC Users 14
UNIX Users 15
Macintosh Users 15
Windows CE Devices 15
Pocket PC Devices 15
SmartPass Version 4.1 New Features 15

Chapter 2 Configuring and Distributing SmartPass for Microsoft Windows **17**
Preparing SmartPass for Installation 17
Configuring the Installation Package 17
FIPS Token (FIPS 140–1) 19
VCAT Token 19
PCAT Smart Card Reader 20
Smarty Smart Card Reader 20
CHIPDRIVE External Smart Card Reader 20
Smart Card Formatting Program 20
RSA SecurID Authentication 21
RADIUS Authentication 21
Entrust Authentication 22
Netrust Authentication 22
Winsock Function Call Interception 22
IPSEC 23
Setting WINS Server Addresses 23

PKI Authentication 24
Browser Configuration 24
Preparing On-Line Registration—Without the Deployability Option 25
OLR Launching Options 25
Branding and Localizing SmartPass Installation Program 26
Detecting and Removing SmartPass 2.2.x Files 26
Detecting Smart Card Removal 27
SmartPass Deployability Option 27
Unattended Operations Feature 28
Developing Exit Routine Capabilities 28

Chapter 3 Installing and Registering SmartPass for Microsoft Windows 29
Installing SmartPass 4.x 29
Setting Your WINS Server Address 30
Launching SmartPass 31
Performing On-Line Registration—Without Using the Deployability Option 32
Authentication Tokens 32
FIPS or VCAT Token 33
Configuring Your Default Authentication Method 33
Formatting Your Smart Card 34
Changing Your Access Code 35
Adding/Changing Your Authentication Key 36
Physical Smart Card Readers 37
Setting Up Your Smart Card Reader 37
Configuring Your Default Reader 38
Formatting your Smart Card 39
Changing Your Access Code 41
Adding/Changing Your Authentication Key 42
RSA SecurID Authentication 42
Configuring SmartPass for RSA SecurID Authentication 42
Launching SmartPass Using RSA SecurID Authentication 43
RADIUS Authentication 45
Configuring SmartPass for RADIUS Authentication 45
Launching SmartPass Using RADIUS Authentication 46
Entrust Authentication 48
Launching SmartPass Using Entrust 48
Performing OLR Using Entrust Authentication 49
Configuring SmartPass for Entrust Authentication 51
Netrust Authentication 53
PKI Authentication 54
Logging On with a PKCS #12 File 54
Logging On With a PKCS #12 File by a New User 56
Adding Additional Servers Using OLR 56
Configuring SmartPass for PKI Authentication 58
Choose or Add a PKCS #12 File 59
The SmartPass User Interface 60
The Toolbar 61

SmartPass Options 61
General Options 61
Confirmation Options 62
Logging Options 63
SmartPass Proxy Options 63
Generic Proxy Options 64
FTP Proxy Options 65
Web Proxy Options 66
SSL Proxy Options 67
Uninstalling SmartPass 68

Chapter 4 SmartPass for UNIX 69
Authentication Methods 69
Installing SmartPass for UNIX 70
Command Line Configuration Variables 71
Performing On-Line Registration 71
OLR Commands 72
Launching SmartPass for UNIX 73
Configuring Your Web Browser 73
Telnet and FTP Configurations 74

Chapter 5 SmartPass for Windows CE/Pocket PC 75
SmartPass CE/Pocket PC Software 75
Windows CE/Pocket PC Devices 76
Authentication Methods 76
SmartPass for Windows CE/Pocket PC Software Requirements 77
Setting Up Your SmartPass for Windows CE/Pocket PC Software 77
Installing and Launching the SmartPass for Windows CE/Pocket PC Software 78
Selecting an Authentication Method 78
FIPS Token Authentication 78
RSA SecurID Authentication 79
Configuring SmartPass for Windows CE/Pocket PC 81
SmartPass for Windows CE/Pocket PC Options 82
Single Port Setting 83
Adding/Changing Your Authentication Key 84
Using SmartPass for Windows CE/
Pocket PC 84
The Toolbar 86

Chapter 6 SmartPass for the Macintosh 87
Hardware and Software Requirements 87
Authentication Methods 87
FIPS and VCAT Token 88
Preparing SmartPass On-Line Registration 88
RSA SecurID Authentication 89
RADIUS Authentication 89
Preparing the SmartPass Software for Distribution 89
General Installation Instructions 90

Installing SmartPass 4.x 90
Enabling Your Authentication Token Types 91
Using a Virtual Token 92
Creating a Virtual Token 92
Opening a Virtual Token 93
Performing On-Line Registration 94
Using RSA SecurID Authentication 95
Using RADIUS Authentication 97
Running Secure Applications 98
Configuration 99
Using a Web Proxy to Navigate a Firewall 99
Configure Using InternetConfig 99
Configure Using Internet Control Panel 100
Using an SSL Proxy 100
SmartPass File Location Information 101
Multiple User Support 101
Performing Other System Functions 102
Backing Up Your Virtual Token 102
Changing Your Virtual Token's Location 102
Uninstalling SmartPass 102
Adding or Changing Your Authentication Key 103
Changing the Default Single Port Proxy on SmartPass for the Macintosh 103

Glossary 105

Appendix A SmartPass Files 113
Detailed Description of setup.ini 113
Option Descriptions of setup.ini 114
Labeling Installation Splash Screen 114
AppName 114
Installation Packaging 114
Packages 114
OLR Launching Options 115
OLRPage 115
Execute 116
ExecutePrompt 116
PortList 117
Detection Options 117
Remove22x 117
DetectCardRemovalInterval 117
Winsock Shim Warning Messages 118
WSOCK32WARNx 118
IPSec WINS Server Setup 118
PrimaryWINSServer 118
SecondaryWINSServer 119
SmartPass Installation Package Files 123

Index 125

Overview

V-ONE Corporation's SmartGate is a leading client/server virtual private network (VPN) security software system with a clearly defined mission: to provide enterprise-level security for network-based users to private information and private TCP/IP application services. SmartGate, distributed worldwide, provides strong user authentication, authorization, management, accounting, encryption, key distribution, and proxy capabilities. SmartGate also provides driver-level IPSec transport functionality in addition to our traditional proxy capabilities. IPSec is a method of encapsulating IP packets (not just TCP sessions) to encrypt and protect data while enroute, not just from modification, but also from examination.

NOTE: IPSec is only available with SmartGate 4.0 and later running on a Microsoft Windows NT server and Windows Client.

Using SmartGate, businesses, public organizations, and governmental agencies of all sizes can deliver fast, cost-effective security solutions to communities of Internet, intranet, and extranet users.

Purpose of This Guide

This guide is designed for the SmartGate Server administrator to manage both locally and remotely the SmartGate Server and their end users' access.

Organization of This Guide

Chapter 1 **Introduction to SmartGate**
Basics of SmartGate System and key SmartGate features.

Chapter 2 **Configuring and Distributing SmartPass for Microsoft Windows**
Instructions for the SmartGate administrator on configuring SmartPass for the Microsoft Windows operating systems before distributing to the end user.

Chapter 3 **Installing and Registering SmartPass for Microsoft Windows**
Instructions for the SmartPass end user on installing SmartPass, performing On-Line Registration (OLR), preparing an authentication token, and utilizing the SmartPass user interface.

Chapter 4 **SmartPass for UNIX**
Instructions on configuring and installing the SmartPass software on UNIX operating systems.

Chapter 5 **SmartPass for Windows CE/Pocket PC**
Instructions on configuring and installing the SmartPass CE/Pocket PC software for Microsoft Windows CE/Pocket PC devices.

Chapter 6 **SmartPass for the Macintosh**
Instructions on configuring and installing SmartPass for the Macintosh; and then performing OLR using a virtual token or logging on using RSA SecurID or RADIUS authentication.

Appendix

Appendix A **SmartPass Files**
Detailed descriptions and examples of the major SmartPass files and their configurable options.

Sources of Help

If you experience any problems with your installation or if you need assistance, please contact V-ONE Technical Support at (888) 220–8663 or (301) 515–5260 for international calls. You may also contact V-ONE Customer Care Support through e-mail at customercare@v-one.com.

Typographic Conventions

This guide uses the following typographic conventions to distinguish user- and system-generated syntax, to identify software components, and to display precautionary messages and other guidance for the administrator/user.

To Show...	We use...	Example
Required data or command keywords	Minion Web bold	type: **vplug**
Data or prompts displayed by the system	Courier	`Password`
Filenames, directory names, program names, hostnames, or IP addresses in text	Courier	the `sgconf.ini` file
Variable parameters or options	Italic	**sagadm -enable *userid***
Choice of options	| (pipe; not typed by user)	`sgateacl=`*`yes`*`|`*`no`*
Keyboard keys	Minion Web small caps	Press ENTER
Items of importance that facilitate installation and use of the software	**NOTE:**	**NOTE:** This process is controlled by values in the `sgconf.ini` file . . .
Issues or instructions that, if not acknowledged or adhered to, could cause a loss of data or pose a serious threat to the security of your system	**WARNING!**	**WARNING!** You must enter an Access Code within 30 seconds . . .
Limitation on use of the software by the Macintosh Operating System	**Macintosh USERS:**	**Macintosh USERS:** Oracle is not supported by the Macintosh OS

Chapter 1

Introduction to SmartGate

The SmartGate System provides application-level data security for public and private networks through the integration of:

- Two-factor user authentication, using both physical smart cards and virtual smart cards (soft tokens).
  - An authentication token that the user *has*
  - An Access Code that the user *knows*
- Access control based on authenticated user identification, independent of IP address.
- Electronic distribution, with user On-Line Registration (OLR).
- Driver-level IPSec transport functionality available on a Microsoft Windows NT SmartGate Server. IPSec is a method of encapsulating IP packets to encrypt and protect data from modification enroute. Encryption and data protection are proxy based for Solaris, Linux, Macintosh, Windows CE, and Pocket PC platforms.
- Application- and system-independent TCP/IP interoperability. SmartGate is compatible with previous systems, mainframes, token rings, ethernets, independent LANs/WANs, and most TCP/IP applications.
- Strong, transparent security for most TCP-based applications.
- Server software that supports Microsoft Windows NT and UNIX operating systems and client software that supports Windows, UNIX, Macintosh, Windows CE, and Pocket PC operating systems.
- Dynamic Configuration that virtually eliminates the need for local configuration by the end user. When launched, SmartPass immediately contacts every SmartGate Server for

NOTE: IPSec is only available with SmartGate 4.0 and later versions running on a Microsoft Windows NT server and Windows Client.

NOTE: For detailed information on IPSec, see Chapter 11, "IPSec," in the *SmartGate Administrator's Guide*.

which the user has an authentication key, requests a current list of the user's access permissions, and establishes secure connections between the user's workstation and the available SmartGate communities.

- Multiple Web and TCP access permission assignment using access control lists (ACL) wildcarding.
- An optional strong encryption standard. Triple DES (Data Encryption Standard) encryption is available for an even higher level of security.

NOTE: For detailed information on ACL wildcarding, see the Appendix C, "ACL Wildcarding," in the *SmartGate Administrator's Guide*.

SmartGate System Components

SmartGate consists of the following basic components (Figure 1–1):

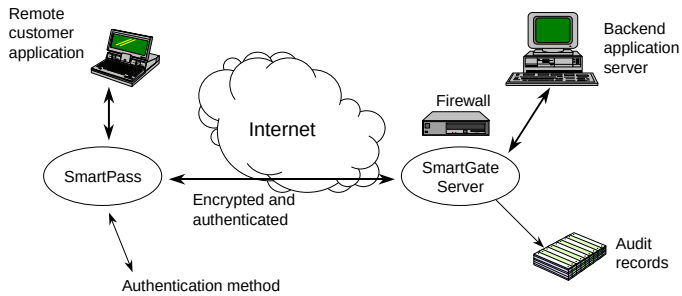


Figure 1–1
SmartGate System

- A SmartGate Server.
- SmartPass software that resides on a user's personal computer.
- An authentication method.
- An Access Code for each authentication token.

SmartGate Server

The SmartGate Server authenticates users and manages access control. It contains an access control database that maps the relationships between users and designated application services. The SmartGate Server allows administrators to assign each user to a SmartGate group, and to apply user- and group-level access privileges to the services that each user may access. On a Microsoft Windows NT Server, they can also assign user- and group-level IPSec access permissions with specific channel types, utilizing the IPSec transport functionality. For example, a site may have users in a "customer" group whose members are permitted access only to an SQL service behind the firewall. Other users may be in the "staff" group, which can access Telnet, POP3, SMTP, and FTP services. Yet, certain users working on a specific project, the "projectX" group, may have access only to an FTP site.

SmartPass Software

SmartPass is SmartGate's client software. It runs on the end user's computer. It manages user authentication and data stream encryption between the user's computer and the SmartGate Server.

Authentication Methods

SmartGate's authentication system supports soft tokens and ISO-standard (physical) smart cards for authentication. A physical smart card is used in conjunction with a smart card reader connected to the user's computer. These methods are:

1. FIPS token (FIPS 140-1 compliant), a virtual token on a smart card or hard drive
2. VCAT token, a virtual token on a smart card or hard drive
3. PCAT reader (accepts MCOS or STARCOS physical smart cards)
4. Smarty reader (accepts MCOS or STARCOS physical smart cards)
5. CHIPDRIVE external reader (accepts STARCOS physical smart cards)

Soft token information may be stored on either the computer's hard drive or a removable disk. The user's SmartGate authentication key is stored on either the physical smart card or soft token and in the SmartGate Server's user database.

Macintosh USERS: Physical smart cards are not supported by SmartPass for Macintosh.

NOTE: The title "MCOS" includes support for both MCOS and MCOS-B smart cards. Use the MCOS card that is pertinent to your network configuration.

SmartGate also supports third-party authentication methods:

- RSA SecurID authentication
- RADIUS authentication
- Netrust authentication
- Entrust authentication
- PKI authentication

Access Code

Each time the user accesses a secure service, an Access Code, similar to a PIN code on an ATM card, is required to unlock the authentication key stored on the user's smart card.

Features of the Access Code include:

- The user can request that SmartPass remember the Access Code for up to 999 minutes. This is the time allowed for session inactivity before SmartPass prompts you for your Access Code.
- The user can suspend his or her Access Code through the SmartPass user interface's "Forget" option. The "forgotten" Access Code must be reentered when the secured session is resumed.

Hardware and Software Requirements for SmartPass

To install SmartPass, most hardware and software requirements depend upon the operating system. However, all user computers must have:

- Internet access
- Connection to a network using TCP/IP protocol
- The appropriate SmartPass software

PC Users

- Microsoft Windows 95, osr2, 95b, 98, 98SE, or Windows NT Workstation, Version 4.0, with service pack 5 or 6a
- Microsoft Windows 2000 (proxy through **localhost** only NO shim support)
- 4 MB of free hard disk space

NOTE: You can check which service pack is installed on your Windows NT machine by clicking **Start**, **Run**, and typing **winver**.

- Netscape Navigator 4.5, 4.51, 4.61, 4.7, 4.72, 4.73 or Microsoft Internet Explorer 5.00, 5.01 (5.01 with service pack 1)

UNIX Users

- A computer with either Sun SPARC Systems running Solaris 2.6 or later; or an Intel (or compatible) system running RedHat Linux 6.0 or 6.1
- 5 MB minimum of free hard disk space
- A suitable UNIX Web browser (must support forms)

Macintosh Users

- An Apple or other Macintosh OS-compatible Power PC computer
- 1 MB of free hard disk space
- Macintosh OS Version 8.1
- Open Transport 1.3

Windows CE Devices

The SmartPass CE software supports the following Windows CE Devices:

- Handheld PC (SH3 and MIPS)
- Handheld PC Professional Edition (SH3, SH4, MIPS, ARM, and StrongARM)
- Palm-size PC (SH3 and MIPS)

Pocket PC Devices

Currently, the Pocket PC software supports the following devices:

- Hewlett-Packard Jornada 545
- Casio Cassiopeia E-115

SmartPass Version 4.1 New Features

- SmartPass/PKI allows SmartPass users to use a PKI certificate in place of other authentication tokens.
- Support for the Towitoko driver, version 2.14.03, has been added.

- In order to ease deployment of SmartPass to end users, navigation of firewalls outside of the SmartGate Administrator's control has been improved to auto-navigate through these firewalls.
- Site-to-Site IPSec enables the SmartGate administrator to set up VPN connections between entire networks via an IPSec tunnel from a SmartGate Server installed on one network to a SmartGate Server installed on another using protocols 50 and 51.
- Smart card removal or replacement causes SmartPass to automatically close all current connections, flush all cached information and shutdown the SmartPass session.

Chapter 2

Configuring and Distributing SmartPass for Microsoft Windows

Preparing SmartPass for Installation

Administrators have the ability to configure SmartPass to reflect a company's organization and structure. The SmartGate administrator should configure SmartPass prior to deploying the software to his end users. Configurable options include the different available authentication tokens and readers, On-Line Registration (OLR) launching capabilities, installation splash screen branding, and desktop icon labeling. Exit routines can also be developed and linked to the SmartPass software. These features are described in detail in the following sections.

Configuring the Installation Package

The SmartPass installation package can be adjusted by the presence of specific authentication options and programs such as the smart card formatting program and the winsock function call interception (shim).

SmartPass currently supports ten authentication options:

1. FIPS token (FIPS 140–1 compliant)
2. VCAT token
3. PCAT reader (accepts either MCOS or STARCOS physical smart cards)
4. Fischer International's Smarty reader (accepts either MCOS or STARCOS physical smart cards)

5. TOWITOKO's CHIPDRIVE external reader (accepts only STARCOS physical smart cards)
6. RSA SecurID authentication
7. RADIUS authentication
8. Entrust authentication
9. Netrust authentication
10. PKI authentication (public key infrastructure)

To individualize your installation package use the `Packages` option in the `setup.ini` file, which is located on the SmartPass installation disk. A standard installation is defaulted to automatically include:

```
Packages=FIPSTOKN,MCOS,SHIM,VCAT
```

Currently, the optional packages are:

FIPSTOKN*	-	FIPS token (FIPS 140–1 compliant) (`fipstokn.z`)
VCAT*	-	VCAT token (`vcat.z`)
PCAT	-	PCAT parallel card reader (`pcat.z`)
SMARTY	-	Smarty card reader (`smarty.z`)
CHIPDRV	-	CHIPDRIVE external card reader (`chipdrv.z`)
CARDFMT	-	Smart card formatting program (`cardfmt.z`)
MCOS*	-	Gemplus MCOS smart cards (`mcos.z`)
STARCOS	-	G&D STARCOS smart card (`starcos.z`)
SGSDI	-	RSA SecurID authentication (`sgsdi.z`)
RADIUS	-	RADIUS authentication (`radius.z`)
SGENTRUS	-	Entrust authentication (`sgentrus.z`)
ENTRUST	-	Entrust authentication (`entrust.z`) The `entrust.z` archive must be created by the administrator with files supplied by Entrust and copied onto the SmartPass installation disk.
SGNETRUS	-	Netrust authentication (`sgnetrus.z`)

NOTE: If both a FIPS and a VCAT token are installed during a new installation, the FIPs token becomes the default. If, however, the user is upgrading with an existing VCAT, the VCAT remains the default. The user can change the default token at any time using the control panel applets.

NOTE: The necessity of individual files are dependant on which authentication method is being used. Please refer to Table A–1 in Appendix A, "SmartPass Files" for a detailed explanation of configuration parameters.

NETRUST - Netrust authentication (`netrust.z`)
The `netrust.z` archive must be created by the administrator with files supplied by Netrust and copied onto the SmartPass installation disk. Please refer to the *SmartGate With Netrust Authentication Guide* for instructions.

SHIM* - Winsock call interception program (`shim.z`)

IPSEC - IPSEC network level security (`ipsec.z`)

BROWSER - Browser configuration (`browser.z`)

PKI - PKI authentication

*Default standard installation package

If your end users are upgrading from a previous version of SmartPass, you must still configure the `Packages` option to include the authentication token they are using. As long as `setup.ini` is configured as previously installed, to include the appropriate token support, upgrading is seamless. The new version of SmartPass will use the existing token. The user does not need to reregister.

FIPS Token (FIPS 140–1)

The FIPS digital token is a software emulation of a hardware authentication token. It stores your private information in an encrypted file system, either on a floppy disk or on your hard drive. A digital or soft token can be used as an efficient and convenient means of authentication, especially when distributing SmartPass to a large number of end users by downloading from a company Web site. During installation, the FIPS token will be automatically placed in the SmartPass directory as the default authentication method and the user will be prompted to format her token. The FIPS token meets the FIPS 140–1 requirements. It is functionally identical to the VCAT, except that a FIPS token can have up to 16 authentication keys on a single token, whereas a VCAT can only have up to 8.

VCAT Token

The VCAT digital token is a software emulation of a hardware authentication token. It stores your private information in an encrypted file system, either on a floppy disk or on your hard drive.

PCAT Smart Card Reader

V-ONE's PCAT parallel smart card reader uses one of the several physical smart cards available to secure and authenticate its users. The PCAT reader is supported by SmartPass for use with either MCOS or STARCOS physical smart cards.

If the smart card formatting program and the `Execute` command have been set in the `setup.ini` file, the user will be prompted during installation to format his physical smart card or he may format it using the control panel applet.

NOTE: PCAT utilization is available to all Windows NT users. However, it must be installed by a user with administrative privileges.

Smarty Smart Card Reader

Fischer International's Smarty reader is supported by SmartPass for use with either MCOS or STARCOS physical smart cards. In the shape of a standard 3.5-inch computer disk, the Smarty reader is easily adaptable for all personal computers. The smart card simply slides into the Smarty reader and then the reader and smart card are inserted in the computer's disk drive.

If the smart card formatting program and the `Execute` command have been set in the `setup.ini` file, the user will be prompted during installation to format his physical smart card or he may format it using the control panel applet.

CHIPDRIVE External Smart Card Reader

TOWITOKO Electronics' CHIPDRIVE external smart card reader is supported by SmartPass for use with STARCOS physical smart cards. It uses the smart card to secure and authenticate its users. This compact reader plugs directly into the CPU's serial port and does not need a battery.

If the smart card formatting program and the `Execute` command have been set in the `setup.ini` file, the user will be prompted during installation to format his physical smart card or he may format it using the control panel applet.

Smart Card Formatting Program

The smart card formatting program is designed to make it easier for the end user to install a PCAT, Smarty, or CHIPDRIVE external reader. One of the ways in which it does this is by hiding from the user the fact that there is both a format code and an Access Code on the MCOS physical smart card. During installation of the SmartPass software, the program will prompt the user for a single code. Both the format code and the Access

Code are set to the code entered by the user. However, this program will only format a smart card if its current format code is set to the default "testcode." If the format code is anything else, the following message will be displayed to the user:

```
This card is not in its initial state.
Please use the Control Panel applet to format it.
```

If the user receives this message, the smart card can be formatted from the control panel applet.

If an MCOS smart card is being used, the applet will prompt the user for the current format code as well as a new format code. The Access Code will then return to its default "pin_code". Whereas, if a STARCOS smart card is reformatted using the control panel applet, the user will be prompted for a new code only and the Access Code will be overwritten by the new code.

The smart card formatting program will also add a corresponding icon to your SmartPass 4.*x* program folder.

RSA SecurID Authentication

The SmartGate System supports a two-factor authentication method using the RSA SecurID token and ACE/Server authentication products developed by RSA Security Inc. SmartGate supports all types of SecurID authentication tokens, including the standard card/key fob, PINPAD card, and SoftID card. The token's microprocessor and host computer are synchronized by a unique number and the time of day. When users log onto an RSA SecurID-enabled host, they are required to type in their Username and passcode, which is a combination of their assigned pincode and the constantly changing number displayed on the token.

NOTE: Detailed configuration instructions for RSA SecurID authentication are presented in "Using RSA SecurID for User Authentication" in Chapter 6, "User Authentication," in the *SmartGate Administrator's Guide*.

WARNING! When using RSA SecurID authentication on a Windows NT SmartGate Server with two network adapter cards, the "default" adapter card cannot be the outside adapter. Using the Windows NT Network Adapter setup, reassign IP addresses to the adaptors.

RADIUS Authentication

RADIUS authentication is an open-standard (RFC 2138) authentication protocol. RADIUS authentication offers secure, easily-passable communication between the client, using the SmartPass software, and the SmartGate Server running the RADIUS module. A shared secret code must be configured into both the RADIUS Backend Server and the SmartGate/RADIUS Server. When users log onto a RADIUS-enabled host, they are required to type in an administrator-provided User ID and password.

NOTE: Detailed configuration instructions for RADIUS authentication are presented in "Using RADIUS for User Authentication" in Chapter 6, "User Authentication," in the *SmartGate Administrator's Guide*.

Entrust Authentication

Entrust authentication provides digital certificates that help create an on-line identification and security system for the Internet. The Entrust authentication method allows SmartPass users to use an Entrust soft token instead of other V-ONE tokens to authenticate. SmartPass and the SmartGate/Entrust Server obtain their credentials from the Entrust Certificate Authority (CA) Server. Each side will validate the other party during the authentication process.

NOTE: Detailed configuration instructions for Entrust authentication are presented in "Using Entrust for User Authentication" in Chapter 6, "User Authentication," in the *SmartGate Administrator's Guide*.

Netrust Authentication

The SmartGate System supports Netrust as an alternative authentication method. Netrust provides digital certificates that help create an on-line identification and security system for the Internet. The Netrust authentication method allows SmartPass users to use a Netrust ready smart card and smart card reader instead of other V-ONE tokens. Both SmartPass and the SmartGate/Netrust Server obtain their credentials from the Netrust Certificate Authority (CA) Server. Each side will validate the other party during the authentication process.

NOTE: Detailed configuration instructions and requirements for Netrust authentication are presented in the *SmartGate With Netrust Authentication Guide*.

Winsock Function Call Interception

By intercepting some of the Windows sockets calls, SmartPass has the ability to eliminate the need for customers to proxy their client applications to `localhost` (`127.0.0.1`). 32-bit applications use the sockets functions exported from the Windows `.dll` file, `wsock32.dll`. Intercepting calls to `wsock32.dll` is accomplished by replacing the system-provided `wsock32.dll` with V-ONE's own `wsock32.dll` and renaming the original as `wsockx.dll`.

WARNING! The Winsock shim does not work if a proxy is being used to traverse a firewall.

The Winsock shim requires that the file `wsock32.dll` (example, the V-ONE version) resides in the Windows system directory and that the original `wsock32.dll` reside in the same directory under the name `wsockx.dll`. The installation program will install the shim components if the archive called `shim.z` is present on the installation disk.

NOTE: Rename this file while the system is running in DOS mode.

If you encounter problems running network applications after installing SmartPass, remove the shim as follows:

```
rename    winsysdir\wsock32.dll wsock32.v1
copy      winsysdir\wsockx.dll wsock32.dll
```

where: *winsysdir* is `\winnt\system32` (Windows NT)
`\windows\system` (Windows 95/98)

The shim intercepts the following winsock calls:

```
inet_addr
asyncgethostbyname
asyncgethostbyaddr
connect
gethostbyname
gethostbyaddr
```

When an application attempts to connect to a SmartGate secured destination, the shim redirects the request to SmartPass.

IPSEC

NOTE: For detailed instructions on IPSec, see Chapter 11, "IPSec," in the *SmartGate Administrator's Guide*.

SmartGate and SmartPass include driver-level IPSec transport functionality. IPSec is a method of encapsulating IP packets (not just TCP sessions) to encrypt and protect the data from modification en-route. V-ONE's implementation also includes support for RFC-standard IP packet payload compression (which compresses the packets before they are encrypted, thus increasing throughput), and Network Address Translation (NAT), as well as a packet filtering engine to implement policy on the traffic flowing in and out of both clients and servers. An IPSEC package is included in the Packages option in the `setup.ini` file. SmartGate 4.0 with IPSec is only available for the Windows NT Server and SmartPass 4.0 with IPSec is only available for Windows 95/98 and the Windows NT Workstation.

Setting WINS Server Addresses

When using IPSec transport functionality, V-ONE recommends that a SmartPass end user configure his or her WINS Server after installing the SmartPass software, but before rebooting the computer. Since SmartPass will be deployed to many different kinds of end users in a variety of situations, the SmartGate administrator is responsible for giving precise instructions to his or her end users.

However, there are two additional IPSec-related options in the `setup.ini` file that can be used to automatically set an end user's WINS Server address during installation of SmartPass. Simply set the options `PrimaryWINSServer` and

`SecondaryWINSServer` to the appropriate IP addresses. These options will automatically overwrite the user's WINS Server address. Consequently, they should be set only if you have a full understanding of your end user's environment, such as, if you are deploying SmartPass to company employees. Whereas, if you are deploying SmartPass to a partner company, so that they may access certain applications within your network, you would not want to set these options.

PKI Authentication

The SmartGate/PKI authentication method allows SmartPass users to use a PKI certificate in place of other V-ONE tokens to be authenticated by a SmartGate Server. The SmartGate Server will continue to use V-ONE's proprietary certificate, and the SmartPass Client will validate that server with an imbedded public key. The SmartPass/PKI Client will then send its PKI certificate (in PKCS #7 form) to the SmartGate/PKI Server for validation. The SmartGate/PKI Server will then validate the certificate by checking for the certificate validity dates and/or checking for a valid signature against a list of signer's certificates that are trusted by the SmartGate/PKI Server. Once the verification is done, the SmartGate activities are identical to that as with any other V-ONE token.

Browser Configuration

The browser configuration package can be installed to make SmartPass change the browser proxy settings on startup. SmartPass 3.4 and earlier included this functionality as part of the base product. In SmartPass 3.4a automatic browser configuration has been made into a separate optional component to increase SmartPass configuration options for the SmartGate Server administrator. The browser configuration package is not needed when installing the shim package and is not included in the default package options.

Preparing On-Line Registration—Without the Deployability Option

NOTE: If you are using a proxy to navigate a firewall, see "Performing OLR Through a Firewall" in Chapter 7, "On-Line Registration Services," in the *SmartGate Administrator's Guide*.

NOTE: For any option to be read, the line must be uncommented.

SmartPass uses a browser-based OLR process. Unless otherwise configured, end users may perform OLR by opening SmartPass and a Web browser and entering the URL `http://your.smartgate.domain:3845/OLR` for single port operations and `http://your.smartgate.domain:2090/30reg.html` for multiple port operations in the browser address field. The browser will display an HTML OLR registration form. The end user must input the required data and click the **register** button. The OLR registration fields, located in the `reginfo.dat` file and the OLR branding options, located in the `sgconf.ini` file, would have been created during configuration of the SmartGate Server via SmartAdmin. See "Setting Up On-Line Registration" or "OLR Branding Options" in Chapter 5, "Using SmartAdmin" for detailed information.

OLR Launching Options

WARNING! If you are using the HTTP (Web or SSL tunneling) Proxy with authorization required, do not use automatic On-Line Registration (i.e., do not enter a Web OLR URL for the `OLRPage` option in the `setup.ini` file, located on your SmartPass installation disk).

The SmartGate administrator may configure the SmartPass installation disk to automatically launch the end user into a specified URL address (i.e., the company OLR page) and/or a specified program following installation and launching of the SmartPass software. There are three settings in the `setup.ini` file, located on the SmartPass installation disk, involved in the OLR launching options:

1. `OLRPage`

   Specifies the On-Line Registration URL, either the standard single port OLR Web page (`http://your.smartgate.domain:3845/OLR`), the multiple port OLR Web page (`http://your.smartgate.domain:2090/30reg.html`), or your manually created OLR Web page, which will be used to perform OLR. For example:

   ```
   OLRPage=http://www.v-one.com:3845/OLR
   ```

2. `Execute`

   Specifies what program to execute following installation and setup of the SmartPass 4.*x* software. For example, the following will cause the OLR process to be invoked:

   ```
   Execute=vspstart -h http://www.v-one.com:3845/
   OLR
   ```

NOTE: If you want to create your own OLR Web page, see "Manual Setup of an HTML Page for On-Line Registration" in Chapter 7, "On-Line Registration Services," in the *SmartGate Administrator's Guide* for detailed instructions.

3. `ExecutePrompt`

   Specifies the text that is displayed in the message prompt that follows installation. There are two options available depending on installation configuration. If the computer needs to restart, the message prompt will be:

   `Would you like to automatically run the ... following the restart of this computer?`

   If the restart is not necessary, the message prompt will be:

   `Would you like to run ... now?`

   For example:

   `ExecutePrompt=SmartPass On-Line Registration`

These features are useful in controlling the end user's registration process by launching them into the OLR process immediately. Since these options are located on the installation disk, they must be configured prior to distribution of the SmartPass software.

Branding and Localizing SmartPass Installation Program

Branding and localization of the SmartPass 4.*x* installation can be performed using standard resource editor tools as provided with both Microsoft Developers Studio or Borland C++. In order to repackage the installation, you will need InstallShield version 3 and, in particular, the packaging program called `ICOMP.EXE`.

The banner located at the top of the SmartPass installation splash screens can be configured with the `AppName` option in the `setup.ini` file on the installation disk. For example:

`AppName=SmartPass 4.0`

Detecting and Removing SmartPass 2.2.*x* Files

Detection and removal of outdated SmartPass 2.2.*x* files can be configured using the `Remove22x` option in the `setup.ini` file which is located on the SmartPass installation CD:

`Remove22x=yes` (not case sensitive)

NOTE: When changing the OLR branding on the SmartGate Server, an administrator may not enter an "*" because of wildcard matching.

WARNING! Any existing SmartPass 2.2.*x* VCATs are also removed.

The installation program will then detect and remove any SmartPass 2.2.*x* programs as part of the installation procedure. There is no default, if any of your end users are using SmartPass 2.2.*x* products, this option must be set to **yes** in order to detect and purge those files.

Detecting Smart Card Removal

NOTE: Frequent card removal detection will impact performance and quickly diminish battery life in battery-powered smart card readers.

Automatic detection of when a user's smart card has been removed or changed from the smart card reader is implemented by configuring the `DetectCardRemovalInterval` option in the `setup.ini` file.

`DetectCardRemovalInterval=`*`# of seconds between polling intervals`* `(10 to 3600)`

Periodically, SmartPass verifies that the smart card is still inserted into the smart card reader and that the serial number of the smart card is the same as the smart card used to log on.

When SmartPass detects the removal or change of an inserted smart card, it stops all current connections (active or idle) and flushes all cached information. SmartPass then displays the start-up dialog box requesting the user to enter an Access Code.

SmartPass Deployability Option

WARNING! Do NOT use the default port settings of 443 or 80 if either a SSL Server or Web Server is running on your SmartGate Server.

Sometimes SmartPass needs to navigate a firewall where, because of a firewall security policy or corporate architecture, it cannot pass traffic. The `PortList=` located in the `setup.ini` file addresses this problem by enabling the SmartGate Administrator to list the port(s) that the SmartPass installation software will use to attempt the firewall navigation.

NOTE: The line length for `PortList` is 1000 characters maximum.

```
PortList=values
```

Once a successful connection is made, the valid port is written into the registry and this port is used for all future connections.

WARNING! Since the 'successful' port is written into the registry, all connections to additional SmartGate Servers must be made on the same 'successful' port.

This option is commented out (in both the `setup.ini` and `sgconf.ini` files) with the default port values being 3845, 443, and 80. The Administrator needs to uncomment the option and verify or insert what ports the SmartPass installation will try to navigate.

Unattended Operations Feature

This feature permits SmartPass to be invoked from an application so that it may run in unattended mode.

Unattended mode is applicable only for VCAT authentication tokens. (The other tokens don't take access code information from the command-line.) Make sure the default authentication method is VCAT before running SmartPass. This is invoked by enabling the check box, **Set as default reader**, on the corresponding control panel applet.

Because of the precedence of parsing command-line input, the *space* is the delimiter by which Windows tokenizes the given input. Thus, it is safe to enclose PIN data with double quotations. That way, even if the access code includes a space (or other special characters), all of the data will be tokenized together. If any of the directories in the path to `smartpass.exe` include a space, the directory path needs to be enclosed with double quotations as well. The following is an example of both the access code and the directory to the executable. The double quotations are required to execute the program successfully.

```
"c:\program files\v-one\smartpass 4.x\
smartpass.exe" -i "PIN=your_access_code"
```

WARNING! If you leave a file that contains your PIN code in an untrusted area, you could compromise the security of your computer and network. A security breach could result from running the `winexec` function call from a `.BAT` file as this exposes your PIN code to viewing or access by others.

Developing Exit Routine Capabilities

To facilitate customer-specific integration efforts, SmartPass can detect and link to user-provided dynamic link libraries that contain functions that will be called at specific points by SmartPass components. These dynamic link libraries are called user exit dll's. Sample source code and additional documentation on developing these libraries are available from the V-ONE Web site (`http://www.v-one.com/`).

Chapter 3

Installing and Registering SmartPass for Microsoft Windows

The following chapter is written for the SmartPass end user. Included are instructions for:

- Installing and launching SmartPass.
- Setting your WINS Server address if necessary.
- Performing On-Line Registration (OLR).
- Configuring your authentication token if necessary.
- Using your SmartPass user interface—including SmartPass Options and Proxy Options.

Installing SmartPass 4.*x*

NOTE: You must log in with administrative rights before installation.

NOTE: Microsoft Windows 2000 supports proxing through **localhost** only, there is NO shim support

NOTE: Your CD-ROM drive may differ depending on your system configuration.

SmartPass runs on Microsoft Windows 95, 98, Windows NT 4.0 or Windows 2000. This section describes installation of SmartPass from a CD-ROM or floppy disk. If you are installing SmartPass from a network download, follow the instructions provided by the download site.

1. Insert the SmartPass installation disk into your a:\drive or your CD-ROM drive (normally d:\), depending on your installation.
2. From your Windows Start menu select **Run**, type in **a:\setup.exe** or **d:\setup.exe**, and click **OK**.

   If you are upgrading from SmartPass 4.*x* to SmartPass 4.*x* and IPSec is included, the install program will request that you manually uninstall SmartPass and reboot before proceeding with the installation. Use the following instructions to uninstall SmartPass manually, otherwise proceed with step 3. Open the Windows **Control Panel**, click

the **Add/Remove Programs** icon, select **SmartPass 4.*x*** from the list, and click **Remove** to uninstall the software. Using the uninstall program will not remove your authentication token. Reboot your computer and run SmartPass' `setup.exe` program.

3. Follow the instructions to complete the installation.

   During a FIPS or VCAT installation, you will be prompted to automatically format your token by entering and confirming a format/Access Code from 4 to 16 characters. This code, if you choose to enter it, will be the new default for both your format and Access Code. Please choose a code that you will remember. You will need this code every time you launch SmartPass and if you ever need to reformat your token.

   During a PCAT, Smarty, or CHIPDRIVE external card reader installation, if the smart card formatting program has been included in the SmartPass installation package, you may be prompted to format your token. However, the physical smart card's format code must be "testcode" for formatting to occur during installation.

4. You may be prompted to reboot your computer at the end of the installation process. Before rebooting, you may want to set up your WINS Server address.

NOTE: An upgrade will install the new version of the SmartPass software into the existing SmartPass.

Setting Your WINS Server Address

You should configure your WINS Server address after installing SmartPass but prior to rebooting your computer. However, your SmartGate administrator may have set up your SmartPass software to automatically configure your WINS Server address. Please check with your SmartGate administrator for further instructions. He or she can tell you if you need to configure your WINS Server and, if you do, exactly how to configure it with the correct address.

For example, you could use the following instructions to configure a Windows NT dialup interface:

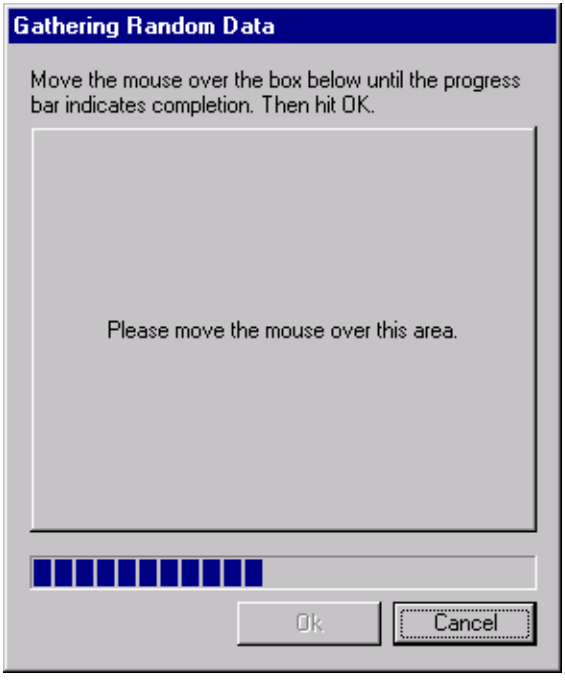
1. To edit the connection properties, run **Dialup Networking** and select which connection you're going to use.
2. Click **MORE** and select **Edit entry and modem properties**.
3. Click the **SERVER** tab.
4. Click **TCP/IP SETTINGS**.
5. Select **Specify name Server Addresses**.

6. Leave all values at zero (0) except for the **Primary WINS** entry—type your **WINS server address**.
7. Click **OK** twice.

Launching SmartPass

When launching SmartPass 4.*x* for the first time, either during a new installation or an upgrade, the program will first prompt you to generate new random data. Figure 3–1 will be displayed on initial startup.

Figure 3–1
Gathering Random Data Window



NOTE: Launching SmartPass procedures differ when using RSA SecurID, RADIUS, or Entrust authentication. Refer to the "SecurID Authentication," the "RADIUS Authentication," or the "Entrust Authentication" section later in this chapter for more information.

Depending on how the SmartGate administrator configured your version of SmartPass, you may be automatically launched into a specific program, such as your Web browser, immediately after launching SmartPass and gathering your random data.

Performing On-Line Registration—Without Using the Deployability Option

SmartPass uses a browser-based On-Line Registration (OLR) process. In order to perform OLR:

- Launch SmartPass
- Open a Web browser
- Enter the URL `http://your.smartgate.domain:3845/OLR` as the browser address or as instructed by your administrator.
- A Web OLR form will appear in the browser. Enter the required data and click **Register**.

WARNING! If your smart card is not preformatted, you will need to format it before performing OLR. Continue with the "Authentication Tokens" section.

NOTE: The URL for the multiple port OLR Web page is `http://your.smartgate.domain:2090/30reg.html`.

Authentication Tokens

SmartPass provides strong token-based user authentication and encryption services. The SmartGate administrator, prior to distribution, will most likely have configured your token type. You will be able, depending on configuration, to format your VCAT during installation of SmartPass, or format your physical smart card for use with a reader. SmartPass currently supports the following token types:

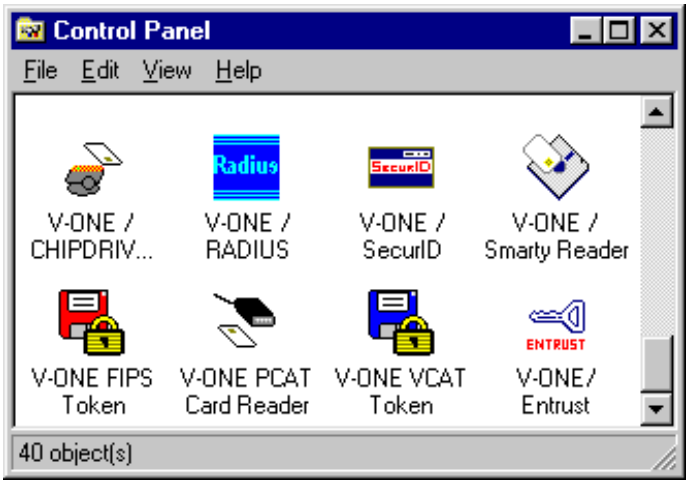
1. FIPS token (FIPS 140–1 compliant)
2. VCAT token
3. PCAT reader (accepts either MCOS or STARCOS physical smart cards)
4. Smarty reader (accepts either MCOS or STARCOS physical smart cards)
5. CHIPDRIVE external reader (accepts STARCOS physical smart cards only)
6. RSA SecurID authentication
7. RADIUS authentication
8. Entrust authentication
9. Netrust authentication
10. PKI authentication

These are described below. If you are not sure which token you should be using, consult your system/network administrator.

NOTE: Detailed configuration instructions and requirements for Netrust authentication are presented in the *SmartGate With Netrust Authentication Guide*.

All authentication tokens can be configured at any time through Windows control panel applets as shown in Figure 3–2.

Figure 3–2
Windows Control Panel



FIPS or VCAT Token

Both the FIPS and the VCAT token are software emulations of a hardware authentication token. They store your private information in an encrypted file system, either on a floppy disk or on your hard drive. FIPS is V-ONE's default token. The VCAT token is functionally identical.

NOTE: A FIPS token has up to 16 authentication keys, whereas a VCAT only has up to 8.

Configuring Your Default Authentication Method

To configure SmartPass to use a FIPS token, open your Windows control panel and double-click the **V-ONE FIPS Token** icon. Figure 3–3 is displayed.

Figure 3–3
FIPS Token
General Information Window

NOTE: If you install both a VCAT and a FIPS token during a new installation, the FIPs token becomes the default. If, however, you are upgrading with an existing VCAT, your VCAT remains the default. The user can change the default token at any time using the control panel applets.

Select the **Set as default reader** check box. If you see additional tabs for **Format**, **Change Code**, and **Key Information**, you are ready to proceed to step 2. Otherwise, click the **Settings** tab. Use the **Browse** button to locate your `User.tkn` file.

Formatting Your Smart Card

If you formatted your smart card during installation you do not need to reformat it. If you did not format it or if you wish to change your format code, open your Windows control panel and double-click the **V-ONE FIPS Token** icon or you may use the pull-down menu under **View** in the SmartPass title bar.

If the three tab items: **Format**, **Change Code**, and **Key Information**, do not appear, the path you have chosen for your token is invalid. Go back to the previous section, "Configuring your Default Authentication Method," and configure the path on the **Settings** tab again. Otherwise, choose the **Format** tab. Figure 3–4 is displayed.

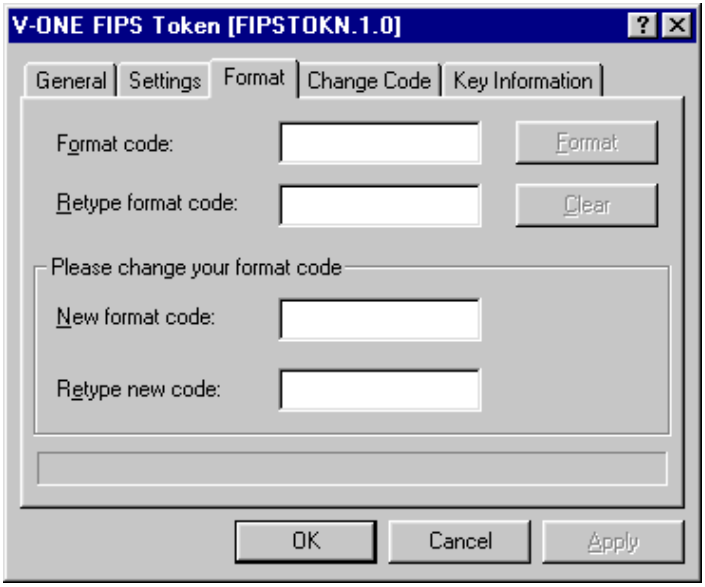


Figure 3–4
FIPS Token
Format Window

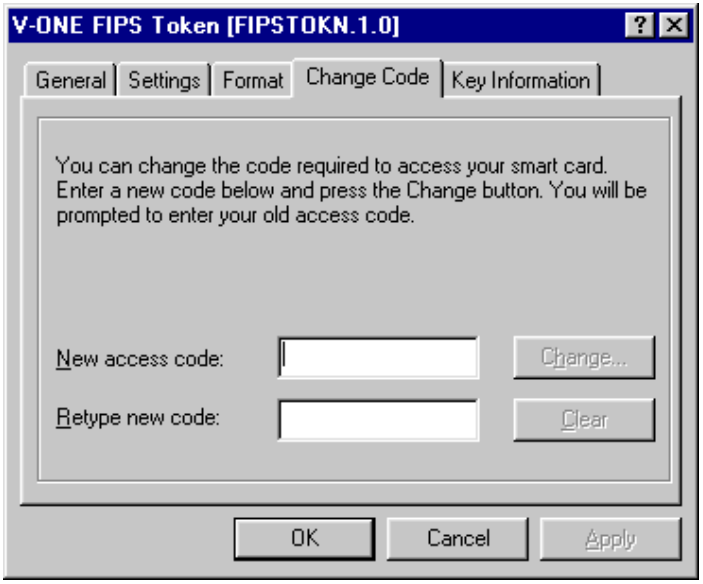
This screen prompts you for the **Format code** and a **New format code**, and confirmation for each. Type the Format/Access Code you entered during installation or the SmartGate default "testcode" if you did not format your token during installation. The new format code is up to you but must be between 4 and 16 characters and should be something you will remember, as you will need it if you ever have to reformat your token. Enter these values and click **Format** to format your token.

WARNING! If you forget your Access Code, you must uninstall SmartPass, manually delete the `V-One` folder from `Program Files`, reinstall SmartPass, and perform OLR again.

Changing Your Access Code

You may want to change the Access Code you entered during installation or you may want to personalize your default Access Code. To change your Access Code, select the **Change Code** tab. Figure 3–5 is displayed.

Figure 3–5
FIPS Token
Change Code Window



WARNING! If you forget your Access Code, you must uninstall SmartPass, manually delete the `V-One` folder from `Program Files`, reinstall SmartPass, and perform OLR again.

Type in your new code. This code is entirely up to you, but it should be something you will remember. Click **Change** to change your Access Code. You will be prompted to enter your old Access Code before the changes can take effect.

NOTE: There is a space between "pin" and "code."

The old Access Code is the one you specified during installation unless you canceled out of that option, in which case the default Access Code for a new virtual token is "pin code."

Adding/Changing Your Authentication Key

If you need to add or change your authentication key, click the **Key Information** tab . The system displays a listing of keynames (Figure 3–6).

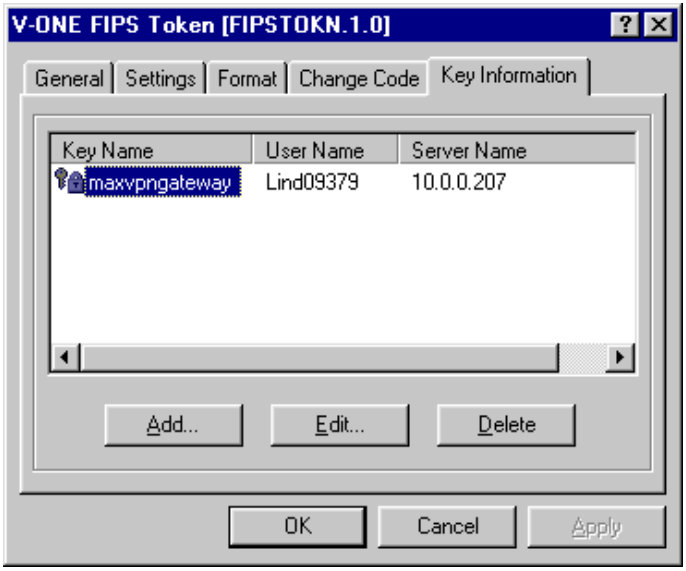


Figure 3–6
FIPS Token
Key Information Window

WARNING! SmartGate uses shared secret key encryption. This means that if a user's authentication key is changed on the SmartGate Server, that user will be unable to access the SmartGate System until the copy of the new authentication key is stored on the user's token (i.e., physical or virtual smart card).

A FIPS token may have up to 16 keynames listed, while a VCAT token may have up to 8. Highlight the appropriate keyname, click **Edit**. Figure 3–7 is displayed.

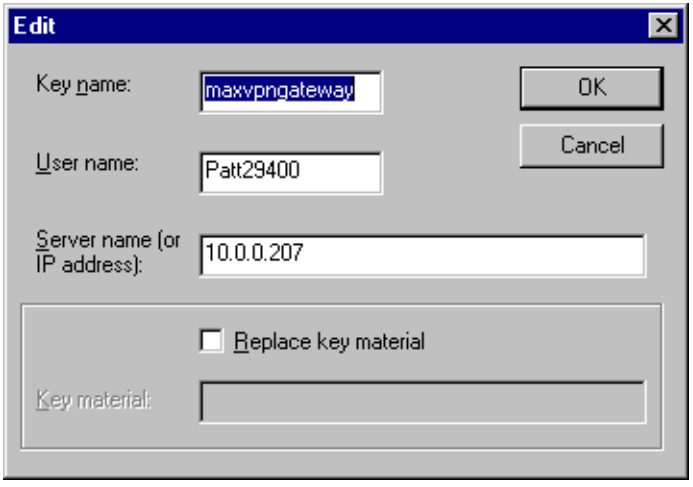


Figure 3–7
FIPS Token Edit Window

Select the **Replace Key Material** check box, type the new authentication key (the 32-bit hexadecimal key), and click **OK**.

Physical Smart Card Readers

SmartPass supports the following physical smart card readers:

1. PCAT reader

   V-ONE's PCAT smart card reader is designed to plug into your parallel port. Your computer must be turned off before plugging in your PCAT reader.

2. Smarty reader

   Fischer International's Smarty reader simulates a standard 3.5-inch computer disk, into which a physical smart card is easily inserted. The Smarty reader is then read from your computer's floppy disk drive.

3. CHIPDRIVE external reader

   TOWITOKO electronics's CHIPDRIVE external smart card reader plugs directly into your serial port.

The PCAT and Smarty readers can use either Gemplus MCOS or G&D STARCOS physical smart cards as their authentication token. However, the CHIPDRIVE reader accepts only STARCOS cards. If the smart card formatting program was included with the SmartPass software by your administrator, you will have the opportunity to format your smart card during installation of the SmartPass software.

Setting Up Your Smart Card Reader

Before you can configure your smart card reader, you must first physically set it up.

- PCAT reader:
  - Make sure the PCAT reader contains a fresh battery.
  - **Turn off your computer** and plug the PCAT reader into LPT1.
  - Insert a smart card fully into the reader with the chip facing up (It should click into the reader).
- Smarty reader:
  - Make sure the Smarty reader contains a fresh battery.
  - Insert your physical smart card into the Smarty reader with the chip facing down, as displayed in Figure 3–8.

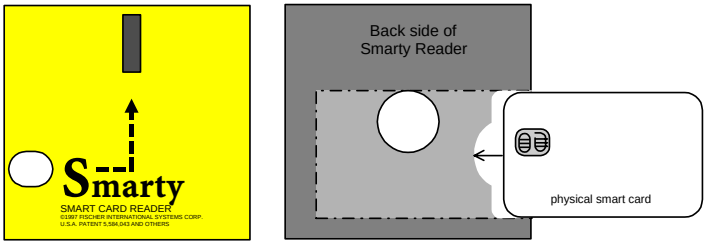


Figure 3–8
Smarty Reader

- Insert the Smarty reader into your computer's disk drive. You may need to press down slightly while inserting to ensure that the magnetic seal in the center of the disk is secure.

■ CHIPDRIVE external reader:

- **Turn off your computer** and plug the CHIPDRIVE external reader into your serial port (RS-232 interface).
- Insert a smart card fully into the reader with the chip end first and facing up (it should click into the reader).

NOTE: The CHIPDRIVE reader accepts only STARCOS smart cards—not MCOS cards.

Configuring Your Default Reader

To configure SmartPass to use your specific card reader, open the Control Panel and double-click either the **V-ONE PCAT Card Reader**, the **V-ONE/Smarty Reader**, or the **V-ONE/ CHIPDRIVE Card Reader** icon. Figure 3–9 is displayed for the PCAT reader. The Smarty and CHIPDRIVE external readers are identical except that the Smarty ready has a **Settings** tab and they all have different titles at the top of the window.

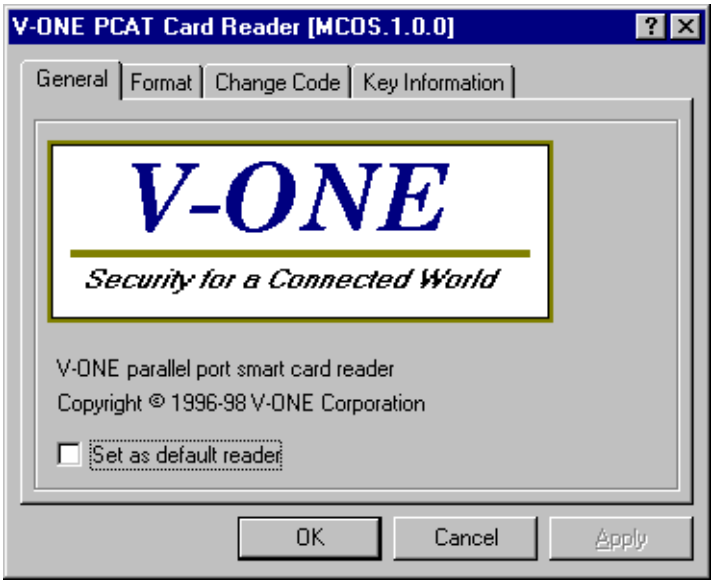


Figure 3–9
PCAT Reader
General Information Window

NOTE: The Smarty reader may pause several seconds while certain actions are processed.

If the control panel applet does not appear or you do not see the **Format**, **Change Code**, and **Key Information** tab items, you will not be able to format your smart card. Return to the previous section, "Setting Up Your Smart Card Reader" and review each of the steps for your smart card reader.

If the applet recognizes your card (example, all the tab items appear correctly), select the **Set as default reader** check box.

The **Settings** tab, available only with the Smarty reader, allows you to set the default drive for use by the Smarty reader. It also allows you to set the reader to "Conserve power." By checking this box, the battery's life will be extended, however, response time will be considerably longer.

Formatting your Smart Card

WARNING! Formatting a smart card erases all existing key information and access permissions on that card.

WARNING! If you reformat your smart card, the new format code will overwrite your existing Access Code. The one exception is if you are using an MCOS smart card and reformatted it using the control panel applet. In this case the Access Code will be reset to the default ("pin code").

NOTE: The smart card formatting option is only available to physical smart cards that have not been previously formatted or if they have been reformatted to their default codes.

If the SmartGate administrator included the smart card formatting program on your SmartPass installation disk, you had an opportunity to format your smart card during installation of the SmartPass software. In so doing, you would have assigned a single code as both Format and Access Code. If you formatted your smart card during installation you do not need to reformat it. You are ready to perform OLR. Please proceed to the section "Performing On-Line Registration" earlier in this chapter.

If you did not format your smart card during installation or if you need to reformat your smart card, open the Control Panel and double-click the appropriate icon for your reader. You may also use the pull-down menu under **View** in the title bar of the SmartPass user interface. Click the **Format** tab.

- Using the Gemplus MCOS smart card with a PCAT reader, Figure 3–10 is displayed. The Smarty reader is identical except for their titles.

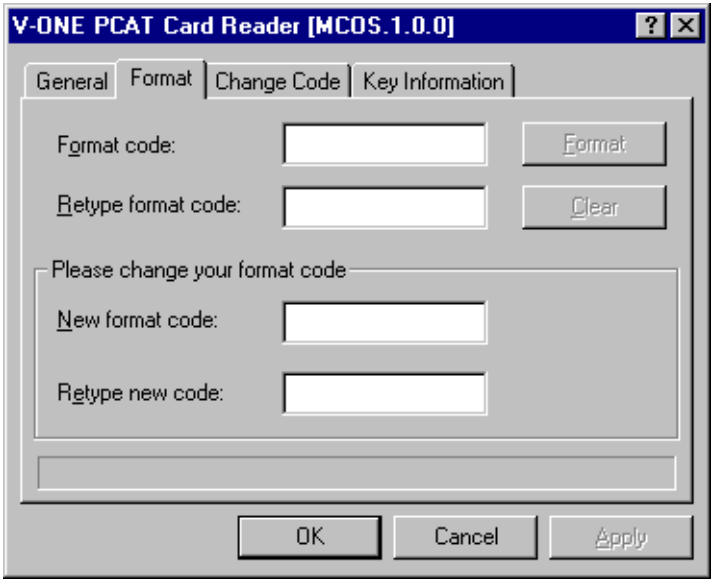


Figure 3–10
PCAT Card Reader
MCOS Smart Card
Format Window

NOTE: CHIPDRIVE readers do not support MCOS cards.

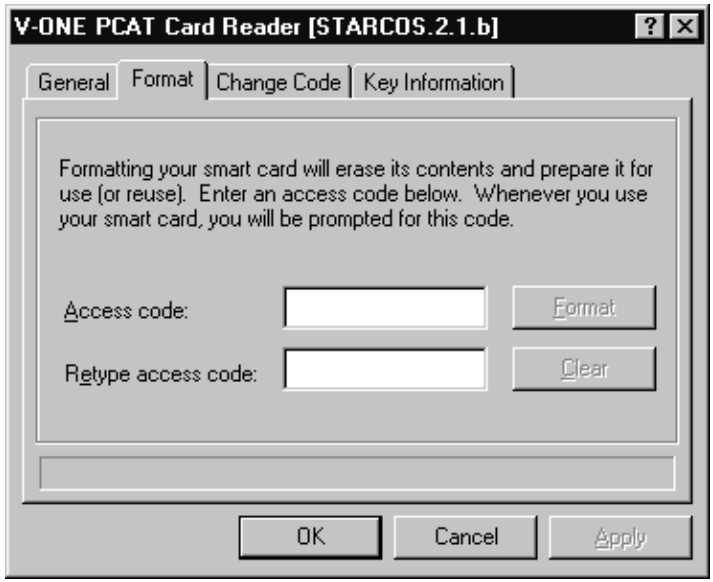
WARNING! If you reformat your **MCOS smart card** using your control panel applet, your Access Code will be reset to the default ("pin code").

This screen prompts you for the **Format code** and a **New format code**, and confirmation for each. Type the format/Access Code you entered during installation or the SmartGate default "testcode" if you did not format your smart card during installation. The new format code is up to you but must be between 4 and 16 characters and should be something you will remember, as you will need it if you ever have to reformat your smart card. Enter these values and click **Format** to format your smart card.

WARNING! If you forget your Access Code, you must uninstall SmartPass, manually delete the `V-One` folder from `Program Files`, reinstall SmartPass, and perform OLR again.

- Using the G&D STARCOS smart card with a PCAT reader, Figure 3–11 is displayed. The Smarty and CHIPDRIVE readers are identical except for the title.

Figure 3–11
PCAT Card Reader
STARCOS Smart Card
Format Window



This screen prompts you to type, then retype as confirmation, a new secret **access code**. Type the Format/Access Code you entered during installation or the SmartGate default "testcode" if you did not format your smart card during installation. The new format code is up to you but must be between 4 and 16 characters. Enter these values and click **Format** to format your smart card. This new code will also serve as your new Access Code, although you may change the Access Code at any time.

WARNING! If you reformat your smart card, the new Format Code will overwrite your existing Access Code. The one exception is if you are using an MCOS smart card and reformatted using the control panel applet, in this case the Access Code will be reset to the default ("pin code").

NOTE: There is a space between "pin" and "code."

WARNING! If you forget your Access Code, you must reformat your smart card. If you also forget your Format Code you must uninstall SmartPass, manually delete the `V-One` folder from `Program Files`, reinstall SmartPass, and re-OLR.

Changing Your Access Code

You may want to change the Access Code you entered during installation or you may want to personalize your default Access Code. To change your Access Code, click the **Change Code** tab. Type your new code and confirmation in the text boxes and click **Change**. The new code is entirely up to you but should be something you will remember. You will be prompted to enter your old Access Code before the changes can take effect. If you formatted your smart card during installation, your old Access Code will be whatever you choose at that time. The default Access Code for a new unformatted smart card is "pin code."

Adding/Changing Your Authentication Key

The last tab, labeled **Key Information**, is used to manually enter authentication key information into your smart card. This will normally be automated through OLR and should not be changed unless specifically requested by your network administrator.

WARNING! SmartGate uses shared secret key encryption. This means that if a user's authentication key is changed, that user will be unable to access the SmartGate System until the copy of the new authentication key is stored on the user's token (example, smart card or VCAT).

RSA SecurID Authentication

The SmartGate System supports a dual-factor authentication method using the RSA SecurID token and ACE/Server authentication products developed by RSA, Inc. RSA SecurID authentication works in conjunction with SmartGate Server 2.4 and SmartPass 3.1 or later versions. SmartGate supports all types of RSA SecurID authentication tokens, including the standard card/key fob, PINPAD card, and SoftID card.

NOTE: When using RSA SecurID authentication, you do not need to perform SmartPass On-Line Registration.

Configuring SmartPass for RSA SecurID Authentication

1. Configure the Default Reader

   To configure SmartPass to use RSA SecurID authentication, open your Windows control panel and double-click the **V-ONE/SecurID** icon. Figure 3–12 is displayed.

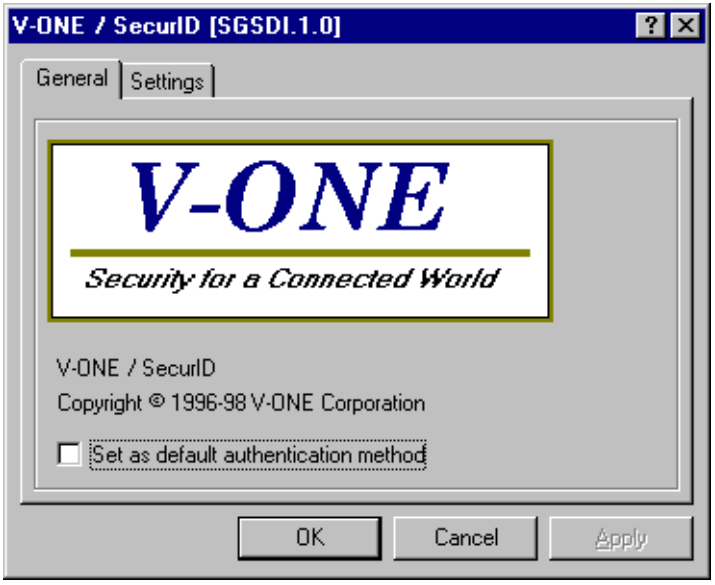


Figure 3–12
SecurID Authentication
General Information Window

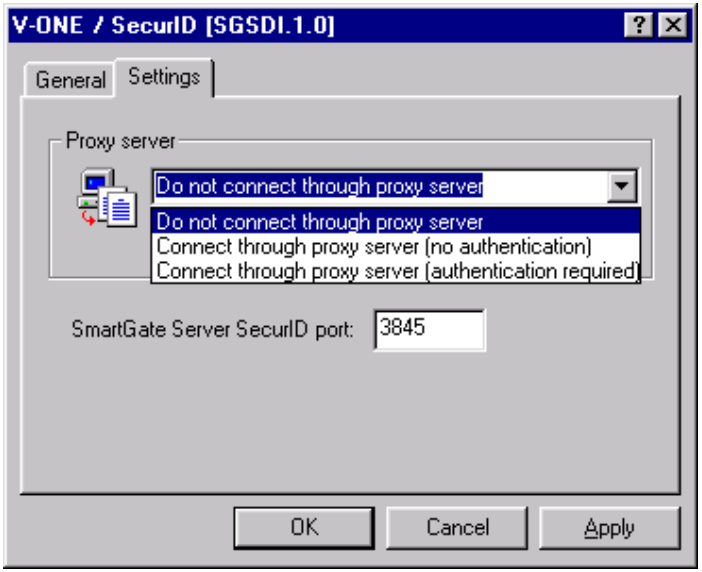
   Select the **Set as default authentication method** check box.

2. Configure RSA SecurID Settings

   Select the **Settings** tab. Figure 3–13 is displayed.

WARNING! Whenusing RSA SecurID authentication on a Windows NT SmartGate Server with two network adapter cards, the "default" adapter card cannot be the outside adapter. Using the Windows NT Network Adapter setup, reassign IP addresses to the adaptors.

Figure 3–13
SecurID Authentication Settings Window



NOTE: The Settings window can also be accessed through the Add SmartGate Server Dialog Box or the Login Dialog Box.

The default setting in the **Proxy server** drop-down box is for no proxy server.

If you need to navigate a simple intermediate firewall, select **Connect through proxy server** and enter the IP address or DNS name of your proxy server and the port number.

If the firewall requires a username/password authentication, select **Connect through proxy server (authentication required)**. You will be prompted to enter the username and password obtained from your system/network administrator. Remember these codes; you will need to enter them every time you open SmartPass. Then enter the IP address or DNS name of your proxy server and the port number.

The **SmartGate Server SecurID port** default is 3845, SmartGate's Single Port Proxy. If you want to connect directly to the SecurID service, use port 2095. If the TCP port was changed in the startup daemon and you are connecting directly, make the corresponding change here.

Launching SmartPass Using RSA SecurID Authentication

When launching SmartPass for the first time using RSA SecurID authentication, the Add Server Dialog Box (Figure 3–14) will prompt the user to enter the hostname or IP address of their assigned SmartGate/SecurID Server.

Figure 3–14
SecurID Authentication
Add Server Dialog Box

NOTE: The hostname/IP address has a 255 character maximum.

Additional servers may be added using the **Add Server** function on the SecurID Login Dialog Box.

The SecurID Login Dialog Box (Figure 3–15) then prompts the user for their **Username** and **Passcode**.

Figure 3–15
SecurID Login Dialog Box

NOTE: The SecurID Login Dialog Box is presented every time SmartPass is launched and each time an authentication has expired.

Enter the Username that identifies you as a user to RSA's ACE/Server. Enter the Passcode, which is a combination of an assigned PIN code and the token code displayed on the RSA SecurID token. The token code is regenerated at timed intervals. SmartPass sends this user information to the SmartGate/SecurID Server, which relays it to the ACE/Server. The ACE/Server performs all RSA SecurID authentications relaying one of three possible responses back to SmartPass via the SmartGate/SecurID Server:

NOTE: The **Passcode** must be a minimum of 6 characters and a maximum of 16 characters.

1. **Success**—The user, identified by their User ID and passcode, has been authenticated.

WARNING! The **Next Code** response must be the token code immediately following the token code submitted in the initial login dialog.

2. **Next Code**—The user must submit the next token code from the token's display. A dialog box similar to the SecurID Login Dialog Box will be displayed, except that the user is only prompted for the next **Tokencode** rather than a **Username** and full **Passcode**.
3. **New PIN**—The user must create a new PIN. There are 3 forms of this response: the user must create his own PIN, accept the server generated PIN, or choose between creating a personalized PIN or using the server generated one. Use the displayed dialog box to enter or accept your new PIN.

Communication between SmartPass and the SmartGate/ SecurID Server is encrypted using standard SmartGate security mechanisms.

RADIUS Authentication

RADIUS authentication works in conjunction with SmartGate Server 2.5 and SmartPass 3.2 and later versions.

Configuring SmartPass for RADIUS Authentication

1. Configure the Default Reader

   To configure SmartPass to use RADIUS authentication, open your Windows control panel and double-click the **V-ONE/ RADIUS** icon. Figure 3–16 is displayed.

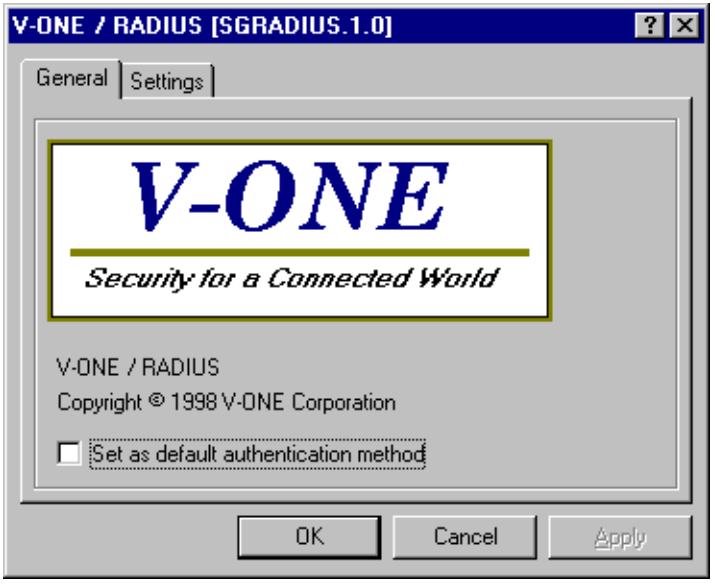


Figure 3–16
RADIUS Authentication
General Information Window

NOTE: When using RADIUS authentication, you do not need to perform SmartPass On-Line Registration.

   Select the **Set as default authentication method** check box.

2. Configure RADIUS Settings

   Select the **Settings** tab. Figure 3–17 is displayed.

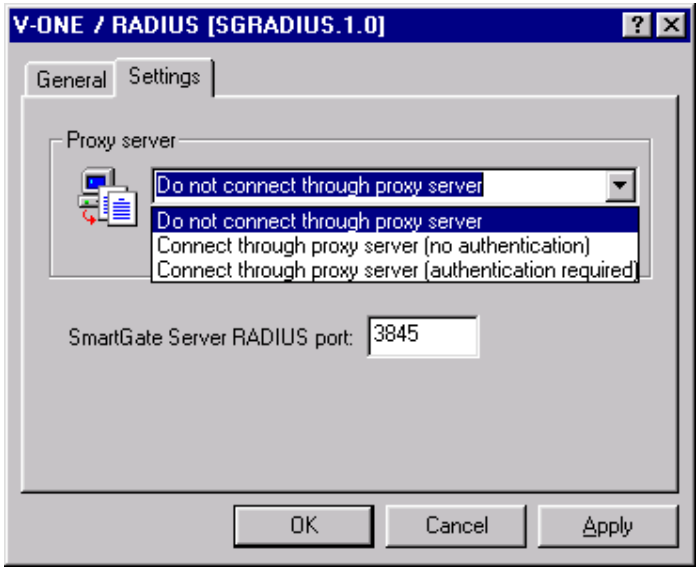


Figure 3–17
RADIUS Authentication Settings Window

NOTE: The Settings window can also be accessed through the Add SmartGate Server Dialog Box or the Login Dialog Box.

   The default setting in the **Proxy server** drop-down box is for no proxy server.

   If you need to navigate a simple intermediate firewall, select **Connect through proxy server** and enter the IP address or DNS name of your proxy server and the port number.

   If the firewall requires a username/password authentication, select **Connect through proxy server (authentication required)**. You will be prompted to enter the username and password obtained from your system/network administrator. Remember these codes; you will need to enter them every time you open SmartPass. Then enter the IP address or DNS name of your proxy server and the port number.

   The **SmartGate Server RADIUS port** default is 3845, SmartGate's Single Port Proxy. If you want to connect directly to the RADIUS service, use port 2097. If the TCP port was changed in the startup daemon and you are connecting directly, make the corresponding change here.

Launching SmartPass Using RADIUS Authentication

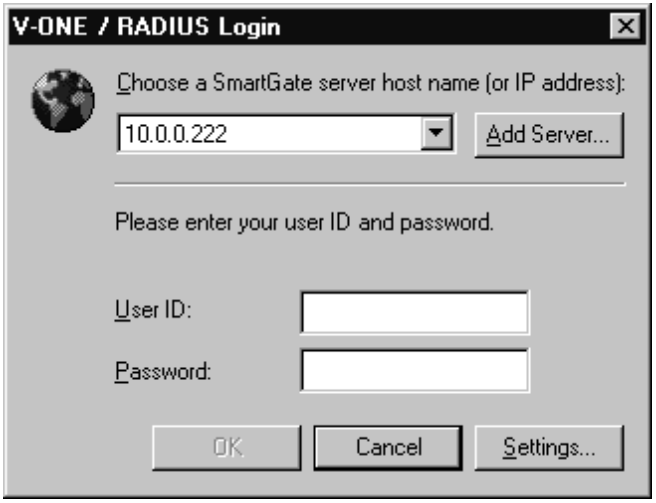
When launching SmartPass for the first time using RADIUS authentication, the Add SmartGate Server Dialog Box (Figure 3–18) will prompt the user to enter the hostname or IP address of their assigned SmartGate Server.

Figure 3–18
Add SmartGate Server Dialog Box

Additional servers may be added using the **Add Server** function on the RADIUS Login Dialog Box.

The RADIUS Login Dialog Box (Figure 3–19) then prompts the user for their **User ID** and **Password**.

Figure 3–19
RADIUS Login Dialog Box



Enter the User ID and Password that identify you as a user to the RADIUS Backend Server. The RADIUS Backend Server performs all RADIUS authentications by relaying one of three possible responses back to SmartPass via the SmartGate/ RADIUS Server:

1. **Success**—The user, identified by their User ID and password, has been authenticated. The SmartGate administrator sets how long each SmartGate session lasts before a new authentication is required.
2. **Failed**—The user has failed to be authenticated. A text message from the server will explain why authorization failed.

3. **Challenge**—The SmartGate/RADIUS Server received a Challenge/Response (Figure 3–20) request from the RADIUS Backend Server. The user must respond to the challenge(s) before they can be authenticated.

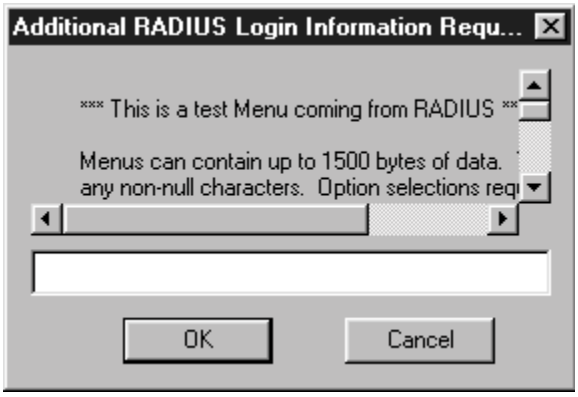


Figure 3–20
RADIUS Challenge/Response Window

NOTE: Challenge/Response is a product of specific programing by the Administrator and consequently may not be used.

Communication between SmartPass and the SmartGate/RADIUS Server is encrypted using standard SmartGate security mechanisms.

Entrust Authentication

Entrust authentication works in conjunction with SmartGate Server 2.7 and SmartPass 3.4 or later versions.

Launching SmartPass Using Entrust

When SmartPass is launched for the first time using Entrust authentication and after gathering random data, the SmartGate/Entrust Login Dialog Box (Figure 3–21) will be displayed.

WARNING! The system time on the Entrust CA Server, the SmartGate/Entrust Server, and the computer where SmartPass is running must be set within 5 minutes of each other.

Figure 3–21
SmartGate/Entrust Login Dialog Box

NOTE: Depending on how your SmartGate administrator configured your SmartPass software you may be launched directly into your OLR Web page.

The first time SmartPass is launched, the only option available in the SmartGate/Entrust Login dialog box will be:

Create an `.epf` File

This is because either:

- you do not yet have an `.epf` file, or
- your SmartGate administrator provided you with one, but it has not yet been linked to your SmartPass/Entrust soft token.

Click **OK** and proceed with the OLR process, which will register you as a user on the SmartGate Server. Perform OLR as specified in the following section.

After at least one `.epf` file has been created, you may choose the `.epf` file corresponding to the SmartGate Server to which you want to connect from the drop-down box. Enter the password you choose during that `.epf` file's creation and click **OK**.

The SmartPass software will be launched and an icon will appear on the right side of your taskbar.

Performing OLR Using Entrust Authentication

SmartPass uses a browser-based registration process. In order to perform OLR:

- Launch SmartPass
- Open a Web browser
- Enter the URL `http://your.smartgate.domain:3845/OLR/entrust` as the browser address or as instructed by your administrator.
- A Web OLR form will appear in the browser. Enter the required data and click **Register**.

Figure 3–22 is an example of an Entrust OLR Web form.

Figure 3–22
SmartGate/Entrust OLR Web Form

- **Registration information**

  The first set of data entry fields were configured by your SmartGate administrator.

- **Use an existing Entrust Profile**

  If your administrator supplied you with an existing `.epf` file, either enter the file name or browse and select the file.

- **Create a new Entrust Profile**

  If your SmartGate administrator did not supply an existing `.epf` file, he will have provided you with a valid Entrust Reference Number and Authorization Code. Enter this information in the fields provided. Create your own Profile Name and Password and enter these values. When SmartPass is launched and every time authentication is required (30 minute default) you must enter your password for the selected `.epf` file.

  Your password must be at least 8 characters long, with a maximum of 32, and no particular character should make

NOTE: Either you will use an existing Entrust Profile or you will create a new one. You do not need to fill out both of these sections.

NOTE: The Profile Name will become the name of your new `.epf` file (i.e., *`profile`*`.epf`).

up half of the password. It must be a combination of both uppercase and lowercase characters. Numbers can be used.

- **Firewall address and port**

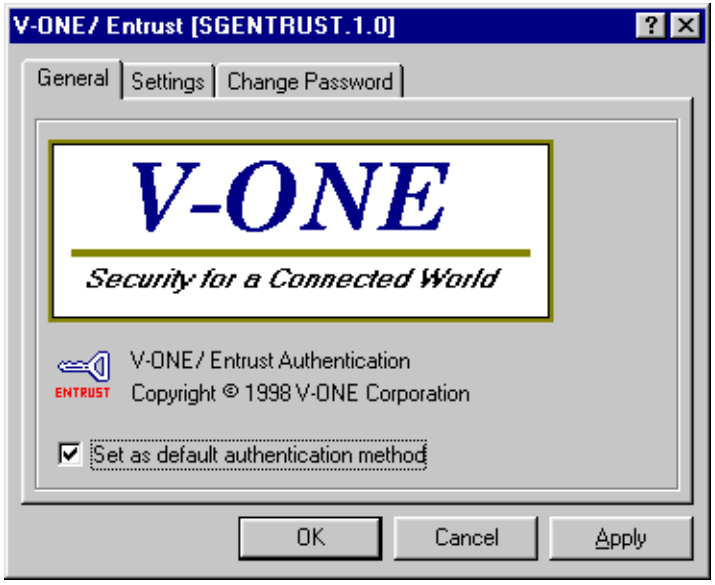
  If you need to navigate an intermediate firewall to exit your system network, enter the firewall's address and port number here.

Configuring SmartPass for Entrust Authentication

1. Configure the Default Reader

   To configure SmartPass to use Entrust authentication, open your Windows control panel and double-click the **V-ONE/ Entrust** icon. Figure 3–23 is displayed.

Figure 3–23
Entrust Authentication
General Window



   Select the **Set as default authentication method** check box.

2. Configure Entrust Settings

   Select the **Settings** tab. Figure 3–24 is displayed.

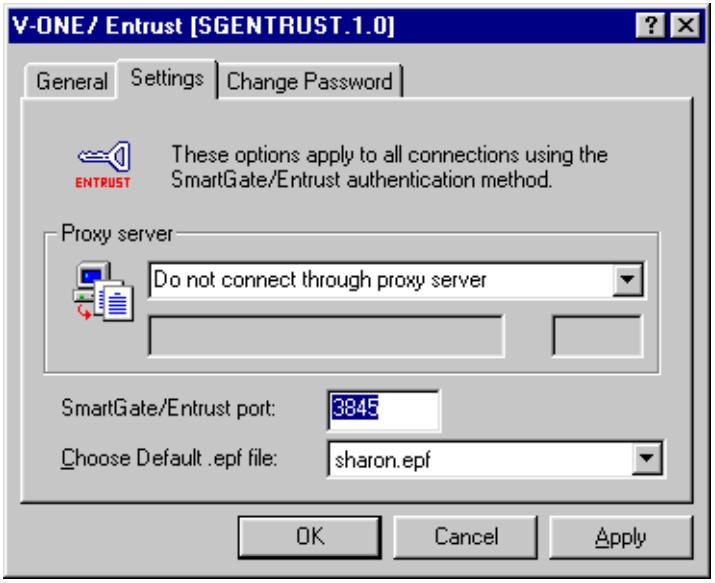


Figure 3–24
Entrust Authentication Settings Window

NOTE: The Settings window can also be accessed through the Login Dialog Box.

The default setting in the **Proxy server** drop-down box is for no proxy server.

If you need to navigate a simple intermediate firewall, select **Connect through proxy server** and enter the IP address or DNS name of your proxy server and the port number.

If the firewall requires a username/password authentication, select **Connect through proxy server (authentication required)**. You will be prompted to enter the username and password obtained from your system/network administrator. Remember these codes; you will need to enter them every time you open SmartPass. Then enter the IP address or DNS name of your proxy server and the port number.

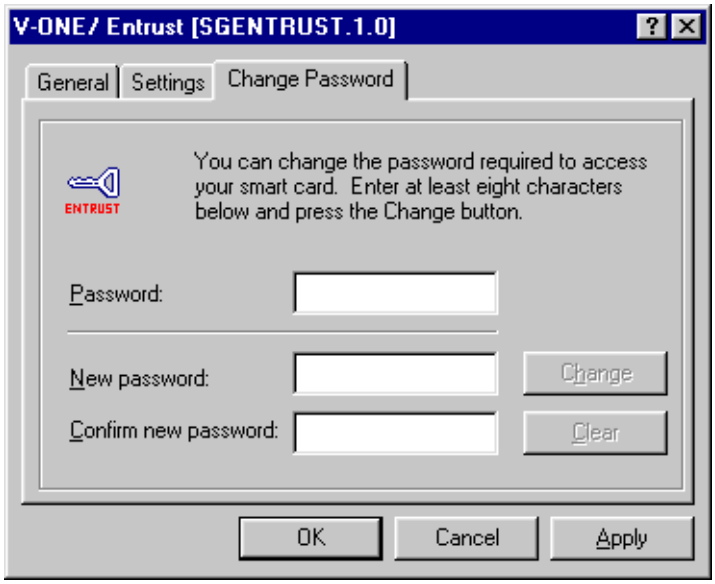
The **SmartGate/Entrust port** default is 3845, SmartGate's Single Port Proxy. If you want to connect directly to the Entrust service, use port 2096. If the TCP port was changed in the startup daemon and you are connecting directly, make the corresponding change here.

Change your default `.epf` file using the **Choose default `.epf` file** drop-down box. If you want to change an `.epf` file's password, it must first be selected as the default.

3. Change Entrust Password

Select the **Change Password** tab. Figure 3–25 is displayed.

Figure 3–25
Entrust Authentication
Change Password Window



If you want to change an `.epf` file's password, it must first be selected as the default in the **Settings** tab.

Type in your old password; then enter and confirm your new password and click **Change**.

The new password should be at least eight characters long and should not be the same as the old password. No particular character should make up half of the password and it must be a combination of both uppercase and lowercase characters. Numbers can be used.

Netrust Authentication

The SmartGate System supports Netrust as an alternative authentication method. Netrust provides digital certificates that help create an on-line identification and security system for the Internet. The Netrust authentication method allows SmartPass users to use a Netrust ready smart card and smart card reader instead of other V-ONE tokens. SmartPass obtains its' credential from the Netrust CA Server during logon.

Please refer to the *SmartGate With Netrust Authentication Guide* for further information on how to configure SmartPass using Netrust authentication.

PKI Authentication

PKI authentication works in conjunction with SmartGate Server 4.1 and SmartPass 4.1 or later versions.

The PKI authentication log on dialog box is displayed:

- When SmartPass is launched
- Every time authentication is required, and the existing authentication context is expired. Presently, this module has 30 minutes of hard-coded time-to-live limit for the authentication context. When the time-to-live has expired and the SmartGate Server requires authentication, this dialog box will automatically appear on user's screen.

The user must choose an existing PKI Certificate File or add one. This file can be located on a floppy or stored on the hard drive.

Logging On with a PKCS #12 File

When SmartPass is launched and the end user is using an existing PKCS #12 file and has already registered to the SmartGate Server via On-Line Registeration, the PKI Login Dialog Box, Figure 3–26, is displayed.

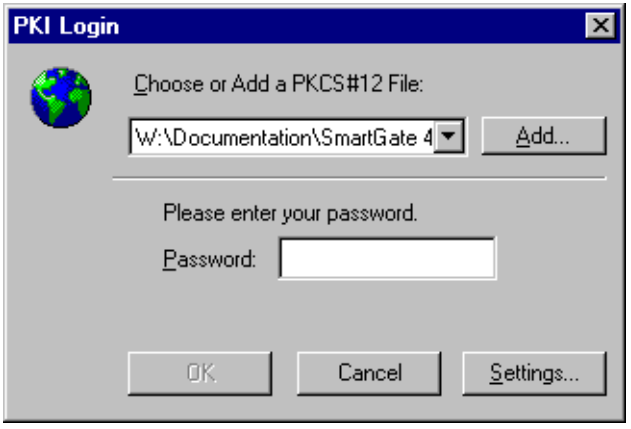


Figure 3-26
PKI Login Dialog Box

The end user just needs to choose an existing PKCS #12 file and enter the valid password. The following is a detailed explanation of the validation/verification process.

1. SmartPass begins the logon process with the PKI token component. The PKI Login dialog box will appear, prompting a user to select a PKCS #12 file (*.p12 or *.pfx) to be used and the corresponding password for the selected

PKCS #12 file. If anything goes wrong during the logon process, an error message box will be displayed to user.

2. The SmartPass/PKI module validates the PKCS #12 file by checking the password validity and/or the certificate's validity dates.
3. If the PKCS #12 file is valid, the SmartPass/PKI module creates a session with each SmartGate Server associated with the PKCS #12 file and submits the authentication request.
4. SmartGate/PKI validates the user's authentication request. The SmartGate Server will check the certificate's validity dates to confirm the certificate is still valid and if the `TrustedCAList` in the SmartGate configuration file (`sgconf.ini`) is set to **yes** and if a trusted CA list exists, it will verify the signature inside the user's certificate by one of the trusted CA certificates. SmartGate/PKI will also verify that the certificate matches the certificate received during OLR. If the `TrustedCAList` in the SmartGate configuration file is set to **no** the SmartGate Server only checks that the dates of the certificate are valid.
5. If the user authentication request is valid, then SmartGate/PKI verifies that the PKCS #7 certificate information for the User ID matches the stored certificate saved during OLR. If the certificates match, then the User ID is considered valid.
6. If the User ID is valid, then SmartGate/PKI creates the second half of the secret key, and requests the SmartGate Authentication Server to update the secret key information for the User ID. The SmartGate Authentication Server updates the user database and replies to the SmartGate/PKI.
7. SmartGate/PKI Server responds to the SmartPass/PKI indicating a successful authentication with a message that contains the second half of the secret key encrypted with the SmartGate Server's private key.
8. SmartPass/PKI decrypts the message, and then creates the full shared key for the session.

These steps are repeated for each SmartGate Server associated to this PKCS #12 file. The result is the list of SmartGate Servers indicating an end of a successful logon process.

NOTE: The PKCS #7 certificate information is enveloped inside the PKCS #12 file.

Logging On With a PKCS #12 File by a New User

1. SmartPass begins the logon process with the PKI token component. The PKI Login Dialog Box, Figure 3–26, appears; prompting a user to select a PKCS #12 file to be used and the corresponding password for the selected PKCS #12 file.
2. If this is the first time the end user is using this PKCS #12 file with this SmartGate Server the following Information screen will be displayed, Figure 3–27.

Figure 3–27
No Server List Information Window

3. If you have already registered to a SmartGate Server you can add the PKCS #12 file via the PKI Control Panel applet, Figure 3–28.

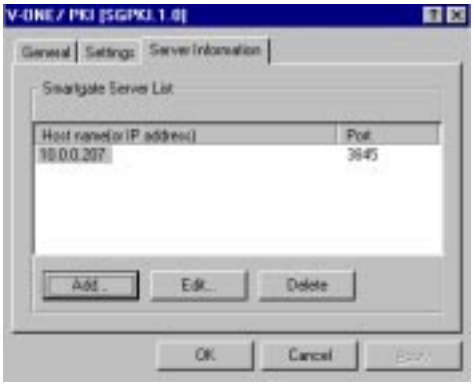


Figure 3–28
Control Panel PKI Server Information Window

NOTE: If you have previously OLRed to this server from another machine, you can add a the server through this window which is located in the Control Panel.

4. Press the **Add** button, select the new PKCS #12 file and enter the password.
5. The User ID will be created, or updated, in the registry and SmartPass will launch with this User ID, with no current servers.

Adding Additional Servers Using OLR

OLR is used to create a new SmartPass/PKI soft-token structure for a user based on a new PKCS #12 file, or registers a current PKCS #12 file to a new SmartGate Server.

The only difference between the two On-Line Registrations is that when a user is using a new PKCS #12 file, the user information is created in the system registry. Then, in both OLRs, an entry will be created in the token for the SmartGate/ PKI server's name and IP address. The entry will contain the necessary information about the server, which will include the server's public key and distinguished name.

SmartPass/PKI uses a browser-based registration process. In order to perform OLR:

1. Launch SmartPass/PKI. The user must logon with a PKCS #12 file and password.
2. Open a Web browser.
3. Enter the URL to the SmartGate Server you want to register to (e.g., `http://smartgate_ip:3845/olr/pki`).
4. A Web OLR form will appear in the browser. Enter the required data and click **Register**. Enter your First Name, Last Name, and the File Name and Password for the PKCS #12 file, Figure 3–28.

Figure 3-28
PKI On-Line Registration Window

5. SmartPass/PKI verifies that the certificate and the password provided by the user are valid and then sends this information to the SmartGate Server.
6. SmartGate returns a successful OLR response with the User ID and one-half of the shared key.
7. SmartPass also updates the token in the system registry.

Configuring SmartPass for PKI Authentication

1. Configure the Default Reader

   To configure SmartPass to use PKI authentication, open your Windows control panel and double-click the **PKI** icon. Figure 3–29 is displayed.

Figure 3-29
Set PKI Default Authentication Window

   Select the **Set as default authentication method** check box.

2. Configure PKI Settings

   Select the **Settings** tab. Figure 3–30 is displayed.

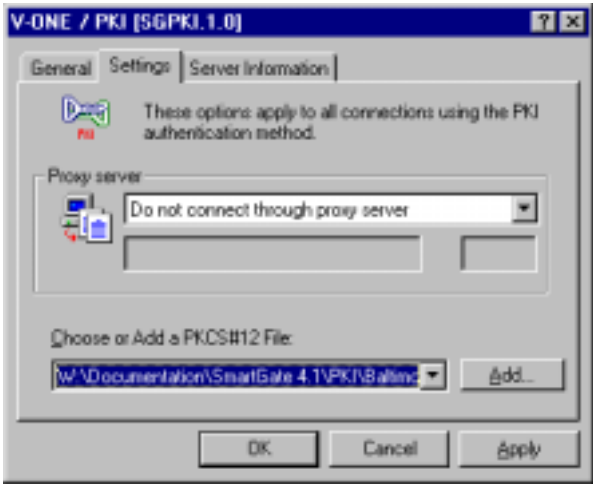


Figure 3-30
PKI Authentication Settings Window

NOTE: The Settings window can also be accessed through the Login Dialog Box.

The default setting in the **Proxy server** drop-down box is for no proxy server.

If you need to navigate a simple intermediate firewall, select **Connect through proxy server** and enter the IP address or DNS name of your proxy server and the port number.

If the firewall requires a username/password authentication, select **Connect through proxy server (authentication required)**. You will be prompted to enter the username and password obtained from your system/network administrator. Remember these codes; you will need to enter them every time you open SmartPass. Then enter the IP address or DNS name of your proxy server and the port number.

Choose or Add a PKCS #12 File

The Settings tab will also allow a PKCS #12 certificate file to be selected or added. If the certificate has never been used before, then it will create a new User ID based on the certificate information.

The SmartPass User Interface

SmartPass typically runs in the Windows taskbar tray. When the display is opened, it looks like Figure 3–31.

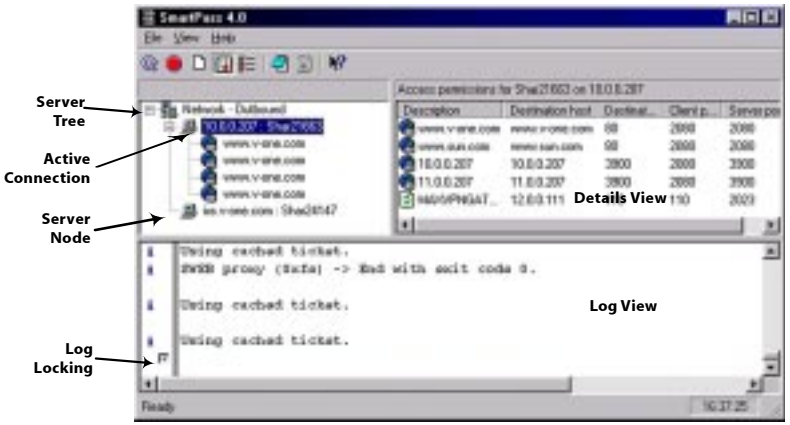


Figure 3–31
SmartPass User Interface Window

NOTE: If you need to reformat your smart card or change your Access Code, you can use the pull-down menu under **View** in the title bar to select the token type being used (your default). This launches you directly into the corresponding control panel applet.

The three views available in the SmartPass user interface:

1. **Server Tree List View**—This pane displays a list of SmartGate Servers for which you have authentication keys. The root node is labeled Network Outbound. Select this node and the Details view will display general information about the operating system, the Winsock version, and your IP address. Branching off the root node are:
   - **SmartGate Server Nodes**—Such nodes appear for each SmartGate Server for which you have an authentication key. Your User ID is also displayed. Select one of these nodes to display a list of your current access permissions for this server.
   - **Active Connection Nodes**—If you have any active SmartPass connections, these appear as child nodes of the SmartGate Server through which the connection was established. Select one of these nodes to display usage details for the currently selected connection.
2. **Details View**—This pane gives you details about whatever item is currently selected in the server list view.

NOTE: If no services are running, the **Shutdown all services** icon will be unavailable.

3. **Log View**—This pane displays the last 100 lines of your real-time activities currently occurring through SmartPass (useful for debugging). Select the check box at the bottom of the screen to "lock" the most recent activities to the bottom of the visible screen.

The Toolbar

The toolbar provides functions for controlling the look and behavior of SmartPass. Each button and its action is briefly described below.


Refresh ACL—Refreshes the access permissions list for each SmartGate Server listed.


Shutdown all services—Closes all connections.


Clear output—Clears the log view information.


Output—Toggles display of the log view.


Options—Displays the SmartPass Options window.


ReadME—Opens the SmartPass ReadME.


SmartPass Log—Opens the entire SmartPass log file.


What's this?—Displays context-sensitive help on user interface elements.

SmartPass Options

The SmartPass Options display provides the ability to configure run-time behavior, such as whether SmartPass should run in the taskbar tray and what kind of logging should be displayed. Proxies and services may have their own configurable options, so you may see additional pages. Open the SmartPass Options display by clicking the **Options** button on the toolbar or by choosing **Options** from the pull-down menu under **View** in the title bar. Select the corresponding tab for each of the following sections.

General Options

The SmartPass Options General Window (Figure 3–32 allows you to configure how often your access control list should be updated through Dynamic Configuration and whether to run SmartPass in the system tray or as a regular Windows application.

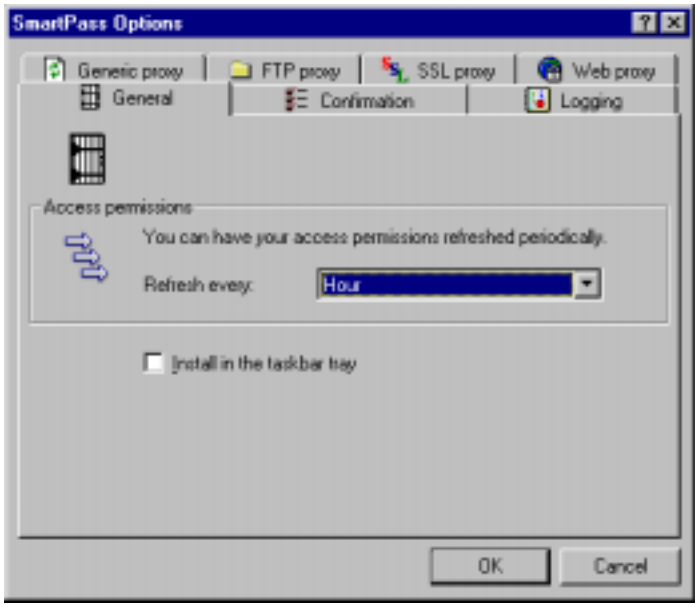


Figure 3–32
SmartPass Options
General Window

Confirmation Options

The SmartPass Options Confirmation Window (Figure 3–33) allows you to configure whether SmartPass should prompt you before taking certain actions, such as shutting down.

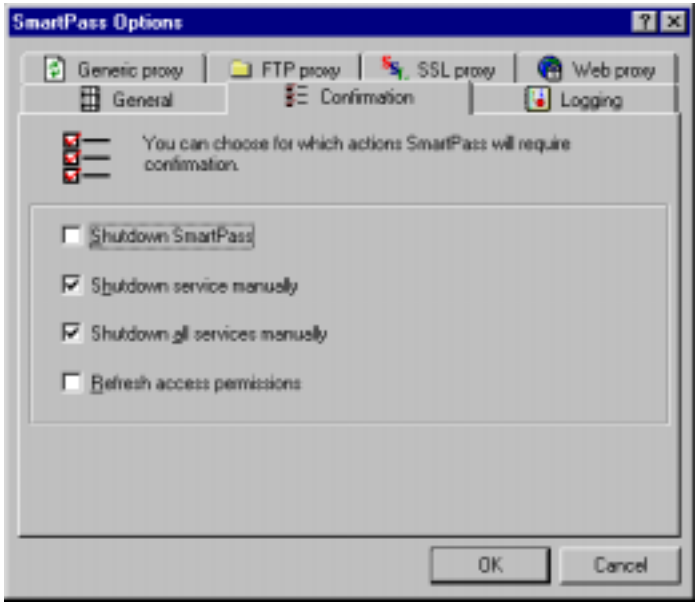
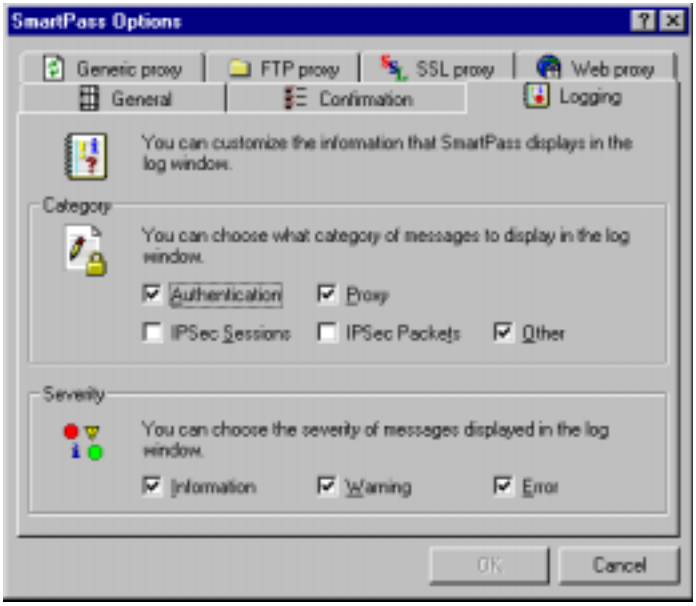


Figure 3–33
SmartPass Options
Confirmation Window

Logging Options

The SmartPass Options Logging Window (Figure 3–34) allows you to configure the log view to display only certain categories and severities of log messages.

Figure 3–34
SmartPass Options Logging Window



SmartPass Proxy Options

If there is a firewall between your client station and the SmartGate Server, you may have to configure SmartPass to successfully negotiate that firewall. If it is a packet-filtering firewall, your network administrator will have to configure it to allow SmartPass transactions through it, but no client configuration will be required. If it is a proxy firewall, the proxies may have to be configured to be aware of the firewall. If you are not sure what your firewall situation is, consult your system/network administrator.

Generic Proxy Options

To configure the Generic Proxy (`sgate`), click the **Generic proxy** tab. Figure 3–35 is displayed.

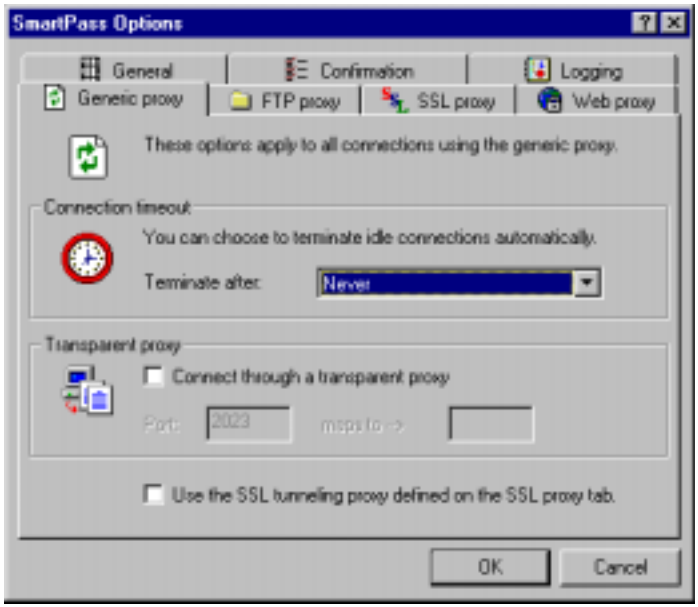


Figure 3–35
SmartPass Options
Generic Proxy Window

The connection can be set to automatically terminate after a designated period of idle time.

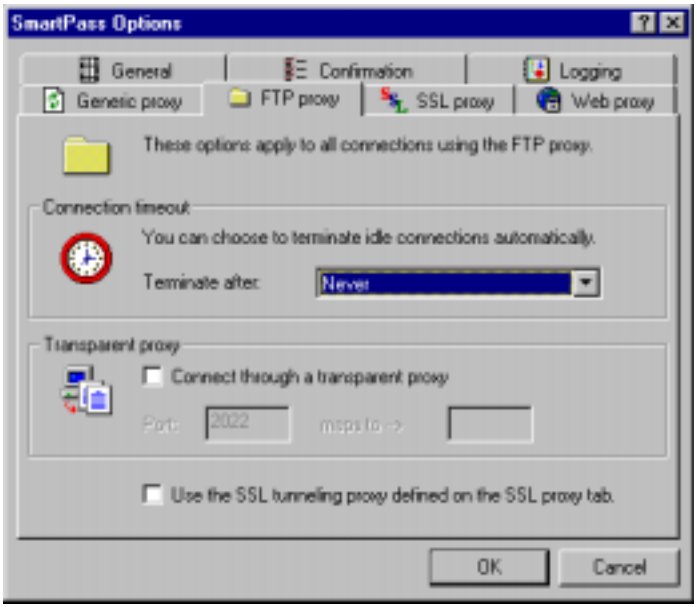
To configure SmartPass to navigate an intermediate firewall, select the **Connect through a transparent proxy** check box. The single port Generic Proxy runs, by default, on port 2023, which displays grayed out. Enter the port of a transparent outbound proxy in the **maps to** text box.

If you want your SmartPass generic sessions to negotiate through an SSL tunneling proxy, select the **Use SSL tunneling proxy defined on the SSL proxy tab** check box. Then define the tunneling proxy on the SSL Proxy tab. Proceed to the section "SSL Proxy Options."

FTP Proxy Options

To configure the FTP Proxy (`spsgftp` and `sgftp`), click the **FTP proxy** tab. Figure 3–36 is displayed.

Figure 3–36
SmartPass Options
FTP Proxy Window



The connection can be set to automatically terminate after a designated period of idle time.

To configure SmartPass to navigate an intermediate firewall, select the **Connect through a transparent proxy** check box. The single port secure FTP Proxy (`spsgftp`) runs, by default, on port 2022, which displays grayed out. Enter the port of a transparent outbound proxy in the **maps to** text box.

If you want your SmartPass FTP sessions to negotiate through an SSL tunneling proxy, select the **Use SSL tunneling proxy defined on the SSL proxy tab** check box. Then define the tunneling proxy on the **SSL Proxy** tab. Proceed to the section "SSL Proxy Options" later in this chapter.

Web Proxy Options

To configure the Web Proxy (sweb), click the **Web proxy** tab. Figure 3–37 is displayed.

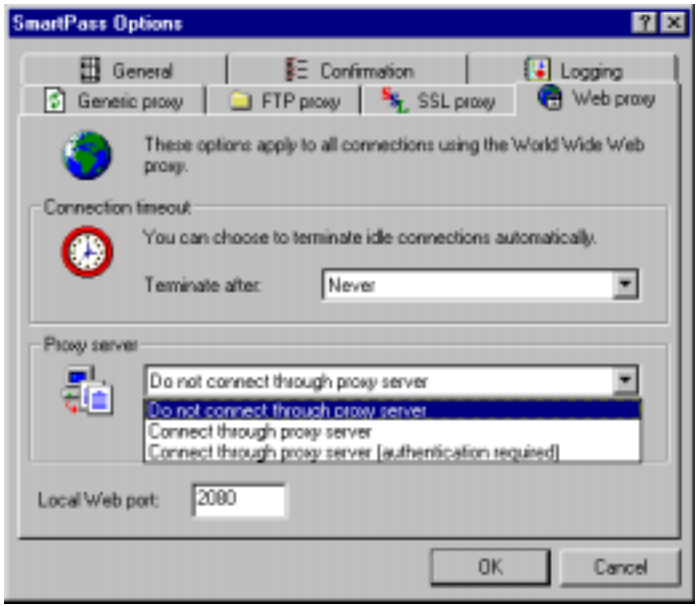


Figure 3–37
SmartPass Options
Web Proxy Window

The connection can be set to automatically terminate after a designated period of idle time.

There are three options available in the **Proxy server** drop-down box:

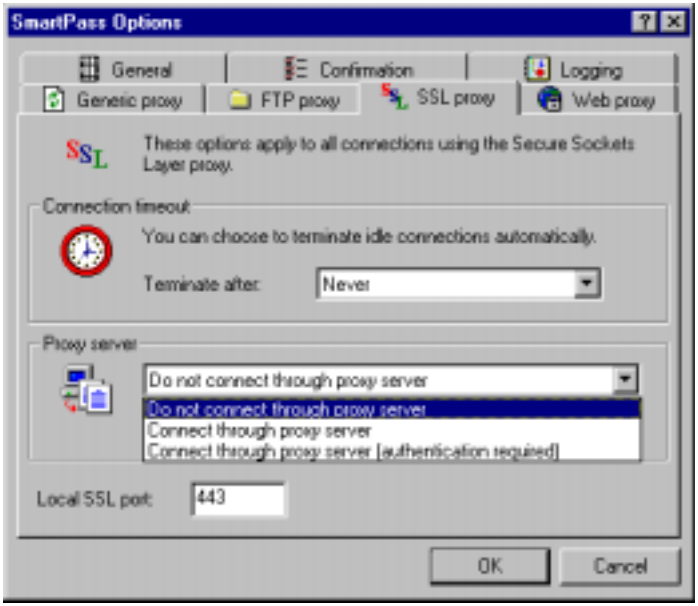
1. **Do not connect through proxy server** is the default setting.
2. **Connect through proxy server** is used to configure SmartPass to navigate a simple intermediate firewall. Select this option and then enter the IP address or DNS name of your Web Proxy server in the large text box and the port in the small text box.
3. **Connect through proxy server (authentication required)** is used to configure SmartPass to navigate an intermediate firewall requiring a username/password authentication protocol. After selecting this option, you will be prompted to enter the username and password obtained from your SmartGate administrator. Remember these codes; you will need to enter them every time you open SmartPass. Then enter the IP address or DNS name of your Web Proxy server in the large text box and the port in the small text box.

While the local Web port is configurable, the Web Proxy default of 2080 is recommended.

SSL Proxy Options

To configure the secure socket layer (SSL) Proxy, click the **SSL proxy** tab. Figure 3–38 is displayed.

Figure 3–38
SmartPass Options
SSL Proxy Window



NOTE: The SSL Proxy requires SmartGate Server software, version 2.4 or later.

NOTE: If you want your generic or FTP sessions to be sent through the SSL tunneling proxy, you must define the proxy here.

The connection can be set to automatically terminate after a designated period of idle time.

There are three options in the **Proxy server** drop-down box:

1. **Do not connect through proxy server** is the default setting.
2. **Connect through proxy server** is used to configure SmartPass to navigate a intermediate firewall. Select this option, then enter the IP address or DNS name of your proxy server in the large text box and the port in the small text box.
3. **Connect through proxy server (authentication required)** is used to configure SmartPass to navigate an intermediate firewall that requires a username/password authentication protocol. After selecting this option, you will be prompted to enter the username and password obtained from your SmartGate administrator. Remember these codes; you will

need to enter them every time you open SmartPass. Then enter the IP address or DNS name of your proxy server in the large text box and the port in the small text box.

While the local SSL port is configurable, the SSL Proxy default of 443 is recommended.

Uninstalling SmartPass

Double-click the **Add/Remove Programs** utility from your Windows Control Panel, select SmartPass 4.*x* from the list, and click **OK**. Reboot after uninstall to complete the process.

It is not necessary to uninstall SmartPass to upgrade if IPSec has not been installed.

Chapter 4

SmartPass for UNIX

NOTE: The deployability option is not available with the UNIX client.

SmartPass for UNIX is available for the Sun SPARC Systems computer running the Solaris 2.6 or later operating system and for Linux (RedHat) 6.0 and 6.1.

Authentication Methods

The SmartPass for UNIX software supports the following authentication methods:

- **FIPS token (FIPS 140-1 compliant)**

  V-ONE's FIPS token is a single-file software emulation of a hardware authentication token. It stores your private information in an encrypted file system. When users open SmartPass, they are required to enter their Access Code. The FIPS token is the system default. If you create a new virtual token, it will be a FIPS token.

With SmartPass for UNIX, you have two options for obtaining your virtual token:

1. Create a new virtual token during On-Line Registration (OLR).
2. Copy onto your UNIX computer an existing virtual token (FIPS) which was created by SmartPass on either a PC or a Macintosh. The Access Code will be what it was defined as on the other computer.

Installing SmartPass for UNIX

There is no installation script for the SmartPass for UNIX software. The files are simply unpacked into a directory of your choice using the **tar** command.

Use the following step-by-step instructions to install the SmartPass for UNIX software. These instructions assume that you want the SmartPass software to reside in a SmartPass directory within your `home` directory. From the Terminal Window:

1. Move to your `home` directory, if you are not already there. Type:

   cd<space>$HOME

2. You may copy or download from the Web the `.tar` file into your `home` directory or you may leave it on a floppy disk or CD-ROM and simply specify its full path and name as the *pathname* mentioned in the next step.

3. Type the command:

   u_sp-<OS>-<Build date>.tar

   For example the UNIX tar file name if built on RedHat 6.0 on July 31, 2000, type:

   u_sp-redhat60-20000731.tar

4. The **tar** command will unpack the SmartPass files into the current directory. This is the SmartPass installation directory and may be used as a permanent location for SmartPass. However, the SmartPass for UNIX files are mobile; they can be moved to any location on your system without affecting the SmartPass software or any other system functions.

   The SmartPass files include:

`ReadMe`	The ReadMe file
`smartpass`	The SmartPass executable
`olr`	The OLR executable

Installation of the SmartPass for UNIX software is complete. You now need to register with a SmartGate Server by performing OLR.

WARNING! When a command is issued, it is also written in your process listing, which lists all current executing processes. Therefore, entering your Access Code using the **-a** command can be a security risk if anyone has access to your computer.

NOTE: When assigning the **LOCAL_PORT_OFFSET,** do not use ports below 1023 or any generally preassigned ports, (example 4000 is used by XWindows).

WARNING! This remote mode is not recommended, since it may be a security risk.

Command Line Configuration Variables

SmartPass for UNIX accepts the following command line variables:

- **-v** Specifies the location of your client's virtual token
- **-a** Specifies your token's Access Code
- **-l** Changes the **LOCAL_PORT_OFFSET** (For example, if the local port offset is 20000 then **localhost** telnet connections to the Extranet client should be set to 20023; default 2000)
- **-s** Single port proxy port number used to connect to the SmartGate Server (default 3845)
- **-f** Firewall proxy which must be traverset to connect to the Internet (For example, 208.0.38.100:80)
- **-r** Allows remote connections to use local SmartPass open ports
- **-d** Prints extra debug information
- **-i** Interactive mode (only used in debugging)

Performing On-Line Registration

SmartPass uses a browser-based OLR process. However, to perform OLR, a separate executable file, named "olr" must be started in the Terminal Window before opening the Web browser.

NOTE: On the UNIX client, SmartPass should not be running during OLR.

1. Run the **olr** executable. From the `SmartPass` directory, type:

   olr

   The following (although version information may differ) will be displayed:

   ```
   olr version 3.1 (c)1999-2000 V-ONE
   Please specify the token name (including path)
   ```

2. Type in the path and name of the token you want to create. If you want it to be created in the `SmartPass` directory, just type the name. For example:

   MyToken

   The following will be displayed:

   ```
   Please specify access code
   ```

3. Type in an Access Code. It must be at least four characters in length and can be any combination of letters and numbers. This code is entirely up to you, but it should be something you will remember. For example, type:

   MyAccessCode

   The following will be displayed:

   ```
   Do you wish to create the new token "MyToken"?
   ```

4. Type: **yes**

   Some diagnostic information may be displayed at first; then the following will be displayed:

   ```
   Listening on port 4090
   ```

   You have now created a new empty FIPS token. Proceed to step 5 to register your new token.

5. Open a Web browser and enter the URL `http://your.smartgate.domain:3845/OLR` as the browser address or as instructed by your administrator.

6. A Web OLR form will appear in the browser. Enter the required data and click **Register**.

   If you must navigate a firewall to access the Internet and have not set its' value with the command line switch -f, enter its' address and port in the **Address** text box.

7. A successful registration Web page should be displayed in the browser window and your Terminal Window will display your destination server

8. Type **Q** to quit.

You are now ready to launch SmartPass.

NOTE: If you want to use an existing token, type in the path and/or name when prompted for the "token path." Then, type the Access Code that was assigned during its creation when prompted for the "access code."

OLR Commands

C, c	Creates a new virtual token
A, a	Changes your Access Code
Q, q	Quits SmartPass (also accepted when SmartPass is running)

Launching SmartPass for UNIX

To start SmartPass:

1. Type:

   smartpass

   The following (although version information may differ) will be displayed:

   ```
   smartpass v3.1(c)1999-2000 V-ONE
   Please specify the token name (including path)
   ```

2. Type the path and name of your token. For example, type:

   $HOME/SmartPass/MyToken

   The following will be displayed:

   ```
   Please specify access code
   ```

3. Type in your Access Code which you assigned your token during OLR. For example, type:

   MyAccessCode

4. SmartPass will obtain your access permissions from the SmartGate Server through Dynamic Configuration and display them in the Terminal Window after you start SmartPass.

NOTE: The location can be specified on the command line using **-v**, and the Access Code may be specified using **-p**.

NOTE: This example uses the UNIX variable `$HOME` to shorten the path name by specifying the user's home directory.

Configuring Your Web Browser

Your Web browser must be set to proxy through **localhost** (**127.0.0.1**) on port **2080** for SmartPass to function. Also, it should be set not to proxy connections to localhost.

There are several different Web browsers that you could be using. The following instructions are for the Web browser, HotJava, since it is included with the Sun Solaris operating system:

1. Open your Web browser
2. Select **Edit** from the Title bar, **Preferences**, and **Proxies**
3. In the **HTTP** text box, type **127.0.0.1**
4. In the **Port** text box, type **2080**
5. In the **Don't Proxy** text box, type **127.0.0.1**

NOTE: SmartPass for UNIX uses single-port only; multi-port connections are not supported.

NOTE: SmartPass for UNIX does not support wildcarded access permissions.

Telnet and FTP Configurations

When using Telnet or FTP the user needs to connect to **localhost** on the port the service is listening.

For example:

If the server redirects telnet and FTP to `10.0.0.230` ports `23` and `21`,

Then (when using SmartPass) the following will be displayed:

```
Listening on port 2023
Listening on port 2021
For destination 10.0.0.230:23 connect to local port 2023
For destination 10.0.0.230:21 connect to local port 2021
```

To Telnet to `10.0.0.230` port `23` the user would type:

```
telnet localhost 2023
```

To FTP to `10.0.0.230` port `21` the user would type:

```
ftp localhost 2021
```

Chapter 5

SmartPass for Windows CE/Pocket PC

SmartPass for Windows CE/Pocket PC is Virtual Private Network (VPN) client software that enables organizations to provide secure remote access to internal networks, applications, and services for employees, customers, and partners using the Microsoft Windows CE and the Pocket PC operating systems.

SmartPass CE/Pocket PC Software

SmartPass for Windows CE/Pocket PC runs on a user's CE device. The SmartPass System manages two-factor user authentication and data encryption between the CE/Pocket PC device and the SmartGate Server.

After installing and configuring the SmartPass CE/Pocket PC software, the user's interaction with the software is limited to entering an Access Code if a virtual token (i.e., a FIPS token) is being used or an RSA SecurID Username and Passcode if SecurID authentication is being used.

The SmartGate Server manages authentication and encryption keys in addition to connection privileges to applications on trusted networks. After a user is authenticated, an encrypted data link is established between SmartPass CE and the SmartGate Server (Figure 5–1). The SmartGate Server then makes connections to private network application servers, based on each user's access permissions (access control list).

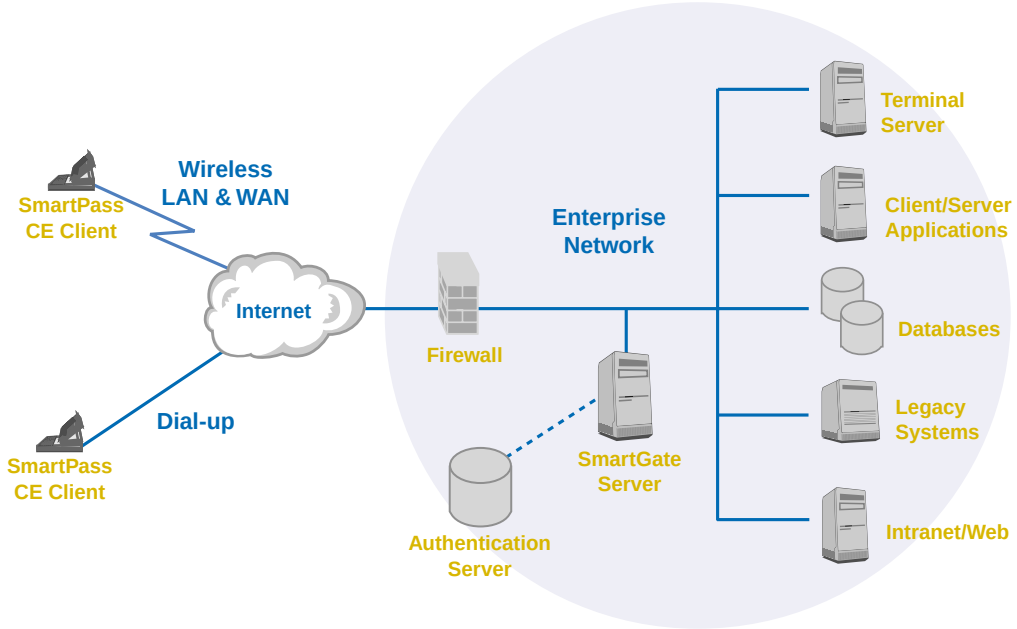


Figure 5–1. SmartPass CE/Pocket PC Network Diagram

Windows CE/Pocket PC Devices

SmartPass CE supports the following Windows CE devices:

- Handheld PC (SH3 and MIPS)
- Handheld PC Professional Edition (SH3, SH4, MIPS, ARM, and StrongARM)
- Palm-size PC (SH3 and MIPS)

SmartPass Pocket PC software supports the following Pocket PC devices:

- Hewlett-Packard Jornada 545
- Casio Cassiopeia E-115

Authentication Methods

The SmartPass for Windows CE/Pocket PC software supports the following authentication methods:

- **Virtual token (FIPS)**

  V-ONE's FIPS token is a software emulation of a hardware authentication token. It stores your private information in an encrypted file system. The FIPS token is in compliance with the FIPS 140–1 coding standards. When users log onto SmartPass using a virtual token, they are required to enter their Access Code.

- **RSA SecurID authentication**

  An authentication method using the RSA SecurID token and ACE/Server authentication products developed by RSA, Inc. The token's microprocessor and host computer are synchronized by a unique number and the time of day. When users log onto a RSA SecurID-enabled host, they are required to type in their Username and Passcode, which is a combination of their assigned pincode and the constantly changing number displayed on the token.

SmartPass for Windows CE/Pocket PC Software Requirements

SmartPass for Windows CE/Pocket PC is installed from computers running Microsoft Windows 95, 98, and NT Workstation 4.0.

Setting Up Your SmartPass for Windows CE/Pocket PC Software

Before installing your SmartPass for Windows CE/Pocket PC software:

1. You must have one desktop/laptop computer.
2. You must have one Windows CE/Pocket PC device, which has an established partnership (serial cable, infrared, or network) with a desktop/laptop computer as displayed in Figure 5–2.

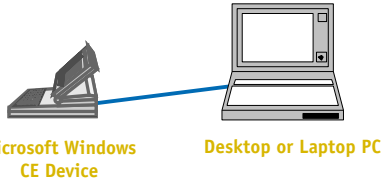


Figure 5–2 Microsoft Windows CE Partnership with a Personal Computer

3. You must have the SmartPass for Windows CE/Pocket PC software. All of the necessary program files reside in one of the following zipped files:

Handheld PC	`spce4hpc.zip`
Handheld PC Pro	`spce4hpcpro.zip`
Palm-size PC	`spce4ppc.zip`
Pocket PC	`spce4pkt.zip`

NOTE: To determine which CE device you have, navigate to **Start, Control Panel, Systems,** and click on the **Systems Tab**.

Installing and Launching the SmartPass for Windows CE/Pocket PC Software

Installation and configuration of the SmartPass for Windows CE/Pocket PC software differs depending on which authentication method is being used. Complete the following steps to install your SmartPass for Windows CE/Pocket PC software; then proceed to the subsection corresponding to your authentication method:

1. Close all open applications on the desktop/laptop computer and the CE device.
2. Establish a partnership between the desktop/laptop computer and the CE device.
3. Copy the appropriate `.zip` file for your CE device to a temporary directory on the desktop/laptop computer and unzip the file.
4. Run Setup.exe on your desktop/laptop computer. This will install the SmartPass CE files into a new directory `\Program Files\v-one\spce,` on the CE device.
5. You will be asked to confirm the installation of the SmartPass for Windows CE/Pocket PC software onto your CE device. Click **Yes**.

Selecting an Authentication Method

FIPS Token Authentication

Use the following steps to set up your SmartPass for Windows CE/Pocket PC software using a virtual token authentication method.

1. Launch SmartPass for Windows CE/Pocket PC on your CE device by clicking **Start**, **Programs**, and then **SmartPass CE**. The FIPS token (virtual token) is the default authentication method, so the FIPS Token Login Dialog Box (Figure 5–3) will be displayed.

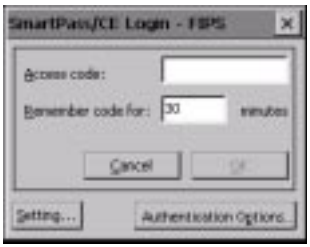


Figure 5–3
SmartPass for Windows CE/ Pocket PC FIPS Token Login Dialog Box

NOTE: If you are upgrading or using an existing token file (`user.tkn`), SmartPass will prompt you for your existing Access Code. Otherwise choose a code that you will remember.

If you are using SecurID as your authentication method, proceed to the section, "RSA SecurID Authentication," for further information otherwise continue with the following steps.

2. When launching SmartPass for Windows CE/Pocket PC for the first time, you will be prompted by an on-screen dialog box for a 4 to 16 character Access Code to your virtual token.
3. Perform On-Line Registration (OLR).
   - Open a Web browser
   - Enter the URL:

     `http://your.smartgate.domain:3845/OLR`
   - A Web OLR form will appear in the browser. Enter the required data and click **Register**.
   - Have your User ID enabled by your SmartGate administrator.
4. After installing and registering your SmartPass CE software, you will need to configure certain settings. Proceed to the "Configuring SmartPass for Windows CE/Pocket PC" section.

Once SmartPass CE is successfully started and configured, it will run transparently with no further interaction by the user.

RSA SecurID Authentication

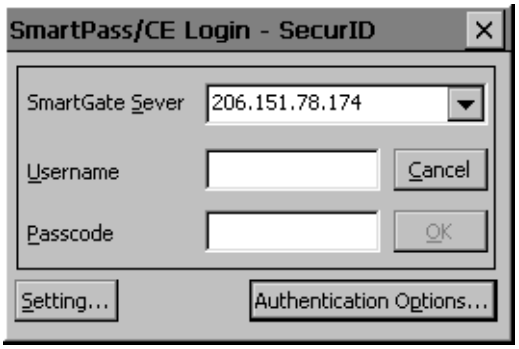
Use the following steps to set up your SmartPass CE software using the RSA SecurID authentication method.

WARNING! Regardless of which authentication method is being used, the HTTP proxy server and e-mail server settings must be manually configured on the CE device or SmartPass will not function.

1. When launching SmartPass CE for the first time, the FIPS Token Login Dialog Box (Figure 5–3) will be displayed by default.
2. To change the default authentication method to RSA SecurID, click the **Authentication Options** button on the FIPS Token Login Dialog Box (Figure 5–4), and select **SecurID Authentication**.

Figure 5–4
SmartPass for Windows CE/Pocket PC Select Authentication Method Dialog Box

3. You will be prompted to enter your Username and Passcode (Figure 5–5).



NOTE: The **Passcode** must be a minimum of 6 characters and a maximum of 16 characters.

Figure 5–5
SmartPass for Windows CE/Pocket PC SecurID Login Dialog Box

- Enter the Username that identifies you to RSA's ACE/Server
- Enter the Passcode, which is a combination of an assigned PIN code and the token code displayed on the RSA SecurID token

The token code is regenerated at timed intervals. SmartPass for Windows CE/Pocket PC sends this user information to the SmartGate Server, which relays it to the ACE/Server. The ACE/Server performs all SecurID authentications, relaying one of three possible responses back to SmartPass via the SmartGate Server:

1. **Success**—The user, identified by his Username and Passcode, has been authenticated.
2. **Next Code**—The user must submit the next token code from the token's display.

WARNING! The **Next Code** response must be the token code immediately following the token code submitted in the initial login dialog.

3. **New PIN**—The user must create a new PIN. There are three forms of this response. The user must create his own PIN, accept the server generated PIN, or choose between creating a personalized PIN or using the server generated one. Use the displayed dialog box to enter or accept your new PIN.

Communication between SmartPass for Windows CE/Pocket PC and the SmartGate Server is encrypted using standard SmartGate security mechanisms.

The first time SmartPass for Windows CE/Pocket PC is started on the CE device, the user will need to configure certain settings. Proceed to the "Configuring SmartPass for Windows CE/Pocket PC" section later in this chapter.

NOTE: SmartPass must be running before opening a secure application.

Once SmartPass for Windows CE/Pocket PC is successfully started and configured, it will run transparently with no further interaction by the user.

Configuring SmartPass for Windows CE/Pocket PC

The following server settings must be manually set on the Windows CE/Pocket PC device.

1. **HTTP proxy server**

   Open your Internet Explorer. From the command bar, click **View**, **Options**, and then the **Proxy Server** tab to configure your HTTP proxy server setting:

   IP address: 127.0.0.1 Port: 2080

2. **E-mail servers**

   Open your Inbox application. From the command bar, click **Services, Options,** and the **Services Tab.** Add highlight POP3 mail, and click **OK** (Figure 5–6).

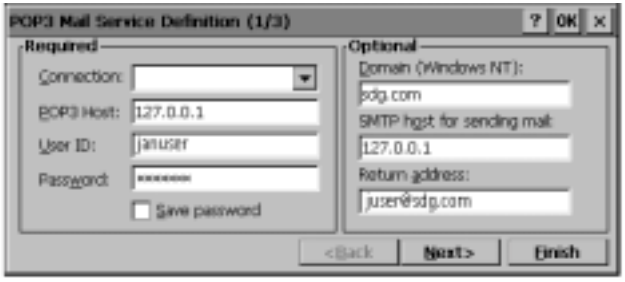


Figure 5–6
SmartPass for Windows CE/Pocket PC
POP3 Mail Service Definition

- **Connection:** Choose the proper or necessary connection (example, LAN, PPP, etc.).
- **POP3 Host:** Specify a new POP3 Host (**localhost** or **127.0.0.1**)
- **User ID** and **Password:** Your mail User ID and Password in the appropriate text boxes
- **Domain:** Your registered domain name
- **STMP (Simple Mail Transfer Protocol) host:** 127.0.0.1
- **Return Address:** Your e-mail address

Click **Next** to finish.

3. **Microsoft Terminal server**

   Open your Terminal Server Client by clicking **Start, Programs**, **Terminal Server Client**, and then the **Terminal Server Client** program (not the wizard). The **Terminal Server Client** dialog box will be displayed.

   In the **Server** text box, type the IP address: **127.0.0.1**

4. **Citrix MetaFrame server location**

   Open your Citrix WinFrame Server Client by clicking the **Start** Menu, **Programs**, **ICA CE Client**, and then **Remote Application Manager**.

   Click the Server Name you want to modify with the correct location. From the command bar, click **Entry** and **Properties**. An information window saying "Searching for Citrix servers" will be displayed. When the connection is complete, the **Select a Citrix Server or Published Application** dialog box will be displayed. Make certain the Citrix Server option button is selected, select an IP address, and click **Server Location**.

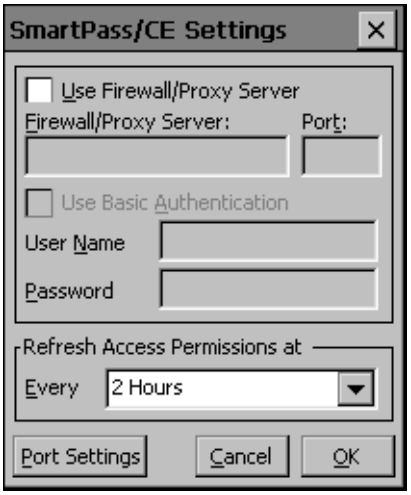
   Click the **Add** button and type the IP address: **127.0.0.1**. Click **OK**.

NOTE: For more information, refer to your Microsoft or Citrix documentation for instructions on configuring the **Microsoft Terminal server** or the **Citrix MetaFrame server location**.

SmartPass for Windows CE/Pocket PC Options

The SmartPass for Windows CE/Pocket PC Settings window (Figure 5–7) can be accessed by clicking the **Options** button on the toolbar or by using the pull-down menu under **Tools** in the SmartPass title bar. It can also be accessed by clicking the **Settings** button on the FIPS Token or the SecurID Login Dialog Box.

Figure 5–7
SmartPass CE Settings

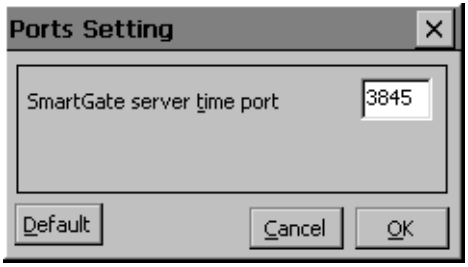


- **Use a Firewall/Proxy Server:** Select this check box if you need to configure SmartPass to navigate a simple intermediate firewall. Enter the IP address or DNS name of your Web Proxy server in the large text box and the port in the small text box.
- **Use Basic Authentication:** Select this check box if you need to navigate an intermediate firewall requiring a username/password authentication protocol. Type in the username and password obtained from your network administrator. Remember these codes. You will need to enter them every time you open SmartPass.
- **Refresh Access Permissions at:** This setting allows you to configure how often your access control list should be updated automatically through Dynamic Configuration.

Single Port Setting

The Port Settings button displays the Port Settings Dialog Box (Figure 5–8).

Figure 5–8
Port Settings Dialog Box



WARNING! Do not change this port unless expressly instructed by your SmartGate administrator.

- **SmartGate server time port:** Allows you to change the time port, which is the default single port proxy setting from the default, 3845, **to a number defined by your SmartGate Server administrator**.

Adding/Changing Your Authentication Key

If you need to add or change your authentication key, click the **Key Information** tab. The system displays a listing of key names (Figure 5–9).

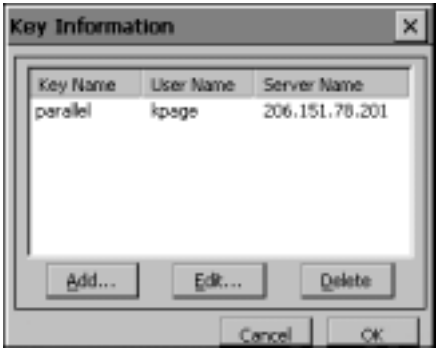


Figure 5–9
Key Information Window

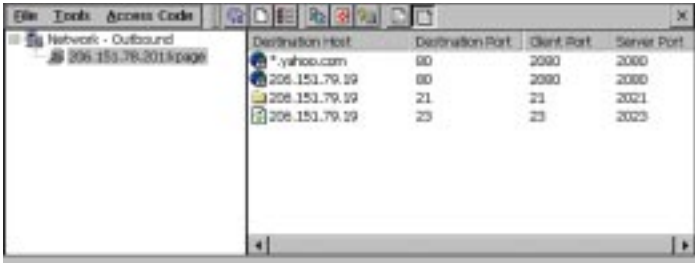
A FIPS token may have up to 16 key names listed. Highlight the appropriate key name and click **Edit**. Select the **Replace Key Material** check box, type the new authentication key (the 32-bit hexadecimal key), and click **OK**.

WARNING! SmartGate uses shared secret key encryption. This means that if a user's authentication key is changed on the SmartGate Server, that user will be unable to access the SmartGate System until the copy of the new authentication key is stored on the user's token (i.e., virtual smart card).

Using SmartPass for Windows CE/ Pocket PC

Launch SmartPass for Windows CE/Pocket PC by clicking **Start**, **Programs**, and then **SmartPass CE**. The SmartPass for Windows CE/Pocket PC user interface (Figure 5–10) will be displayed.

Figure 5–10
SmartPass for Windows CE/ Pocket PC User Interface



The Server Tree and the Details views are displayed by default. You can switch to Log view by clicking the log button.

1. **Server Tree List View**—This pane displays a list of SmartGate Servers for which you have authentication keys. The root node is labeled Network Outbound. Select this node and the Details view will display general information about the operating system, the Winsock version, and your IP address. Branching off the root node are:
   - **SmartGate Server Nodes**—Such nodes appear for each SmartGate Server for which you have an authentication key. Your User ID is also displayed. Select one of these nodes to display a list of your current access permissions for this server.
   - **Active Connection Nodes**—If you have any active SmartPass connections, these appear as subnodes of the SmartGate Server through which the connection was established. Select one of these nodes to display usage details for the currently selected connection.
2. **Details View**—This pane gives you details about the item that is currently selected in the Server List view.
3. **Log View**—Click the SmartPass Log button to display the Log view. This shows the last 100 lines of your real-time activities currently occurring through SmartPass (useful for debugging).

The Toolbar

The toolbar provides functions for controlling the look and behavior of SmartPass. Each button and its action is briefly described below.

Refresh Access Permissions: Refreshes the access permissions list for each SmartGate Server listed.

Clear Log: Clears the log view information.

Settings: Displays the SmartPass CE window.

Change Access Code: Changes your Access Code.

Forget Access Code: Clears your Access Code. The access Code must be reentered for next secure connection.

Key Information: Displays Key Information dialog box.

SmartPass Log: Toggles display of the Log view.

Access Permission View: Displays default user interface view (Server Tree List and Details View).

Chapter 6

SmartPass for the Macintosh

NOTE: If you have a Macintosh with a 68K processor, you must use SmartPass 2.3.1.

Hardware and Software Requirements

SmartPass 4.0 for the Macintosh requires:

- An Apple or other Macintosh–compatible Power PC computer
- Macintosh Version 8.1 or later
- Open Transport 1.3 or later
- Open Transport TCP/IP (MacTCP is NOT supported)
- Either Internet access or a LAN connection using TCP/IP
- A Web browser capable of handling HTML forms
- 1 megabyte of available space on the hard drive of the personal computer on which you will install the SmartPass software.

Authentication Methods

SmartPass for the Macintosh supports the following authentication methods:

- Virtual tokens (FIPS or VCAT)
- RSA SecurID authentication
- RADIUS authentication

All methods can run simultaneously on the same computer, with multiple instances of each method.

FIPS and VCAT Token

V-ONE supports two different virtual tokens:

1. FIPS (SmartPass authenticator) is the new single-file virtual token which is FIPS 140–1 compliant. It is the SmartPass default authentication method unless an upgrade is being performed and a VCAT already exists on that machine. It is functionally identical to the VCAT.
2. VCAT is a folder token containing several files.

V-ONE's virtual tokens are software emulations of a hardware authentication token. Your private information, including your authentication key, is stored in an encrypted file, either on a floppy disk or on your hard drive. A virtual token can be used as an efficient and convenient means of authentication, especially when distributing SmartPass to a large number of end users by downloading from a company Web site.

The content of Macintosh virtual tokens are identical to the Windows versions. Consequently, the same virtual token can be used on both systems; that is, if the token is stored on a floppy disk, the Macintosh system has a 1.4-megabyte floppy drive, and suitable software (example, Apple's PC Exchange).

NOTE: A VCAT created by SmartPass for Macintosh version 3.3 cannot be used on earlier versions of SmartPass.

Preparing SmartPass On-Line Registration

When using a virtual token, SmartPass for Macintosh uses a browser-based On-Line Registration (OLR) process. End users begin the registration process by opening SmartPass and their browser, and entering the following URL in the browser address field:

`http://smartgate.your.domain:3845/OLR`

An OLR form in HTML format, created by the SmartGate Server, will be displayed. End users enter the required data and click **Register**.

The OLR registration form produced by the SmartGate Server can be configured using SmartAdmin. See, "Setting Up On-Line Registration" in Chapter 5, "Using SmartAdmin," in the *SmartGate Administrator's Guide*, for more information.

NOTE: If you want to create a custom OLR registration form, see "Manual Setup of an HTML Page for On-Line Registration" in Chapter 7, "On-Line Registration Services," in the *SmartGate Administrator's Guide*, for detailed instructions.

NOTE: The URL for the multiple port OLR Web page is `http://your.smartgate.domain:2090/30reg.html`.

NOTE: Ignore any fields related to firewalls. See the "Configuration" section for details on specifying firewall proxies.

RSA SecurID Authentication

NOTE: Detailed SmartGate configuration instructions for RSA SecurID authentication are presented in "Using RSA SecurID for User Authentication" in Chapter 6, "User Authentication," in the *SmartGate Administrator's Guide*.

The SmartGate System supports a two-factor authentication method using the RSA SecurID token and ACE/Server authentication products developed by RSA, Inc. SmartGate supports all types of RSA SecurID authentication tokens, including the standard card/key fob, PINPAD card, and SoftID card. The token's microprocessor and host computer are synchronized by a unique number and the time of day. When users log onto a RSA SecurID-enabled host, they are required to type in their Username and passcode, which is a combination of their assigned pincode and the constantly changing number displayed on the token. RSA SecurID authentication works in conjunction with SmartGate Server 2.4 and SmartPass for Macintosh 3.2 and later versions.

RADIUS Authentication

NOTE: Detailed SmartGate configuration instructions for RADIUS authentication are presented in "Using RADIUS for User Authentication" in Chapter 6, "User Authentication," in the *SmartGate Administrator's Guide*.

RADIUS authentication is an open-standard (RFC 2138) authentication protocol. RADIUS authentication offers secure, easily-passable communication between the client, using the SmartPass software, and the SmartGate Server running the RADIUS module. A shared secret code must be configured into both the RADIUS Backend Server and the SmartGate/RADIUS Server. When users log onto a RADIUS-enabled host, they are required to type in an administrator-provided User ID and password. RADIUS authentication works in conjunction with SmartGate Server 2.5 and SmartPass for Macintosh 3.3 and later versions.

Preparing the SmartPass Software for Distribution

When delivered from V-ONE, the SmartPass software includes all authentication methods and is suitable for distribution without the need for any customization. If you intend for end users to download the software using a Web browser, you should save the self-extracting archive on the server in binhex format (file extension .hqx), which will enable a properly-configured browser to decompress the software automatically.

General Installation Instructions

To use SmartPass for Macintosh you must:

1. Install the SmartPass software
2. Enable your token type(s)
3. Create and open your virtual token, and then perform On-Line Registration (virtual token users only)
4. Designate a SmartGate Server and logon (SecurID and RADIUS authentication users only)

Installing SmartPass 4.*x*

If you are upgrading from an earlier version of SmartPass, install the software as specified below. SmartPass will use your existing virtual token and `Preferences` files.

To install SmartPass:

- Decompress the software if necessary.
- Double-click the **SmartPass Installer** icon and follow the on-line instructions through the screens.
- By default, the installer creates a folder called `SmartPass Folder` to store the SmartPass files, but you will have the option to install the software to a different location. (Figure 6–1).

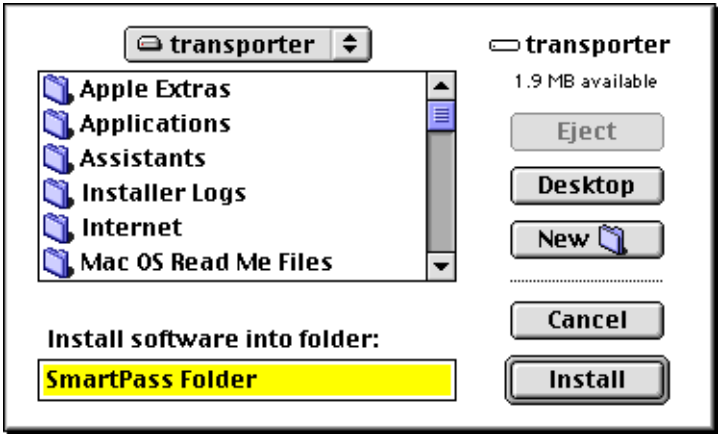


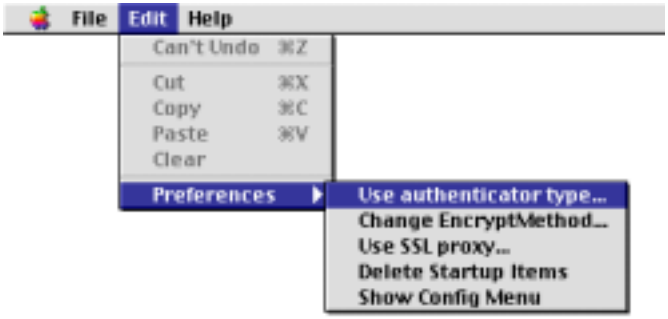
Figure 6–1
SmartPass Installer Window

- You may be prompted to reboot your computer at the end of the installation process.
- Double-click the **SmartPass** icon to start the software.

Enabling Your Authentication Token Types

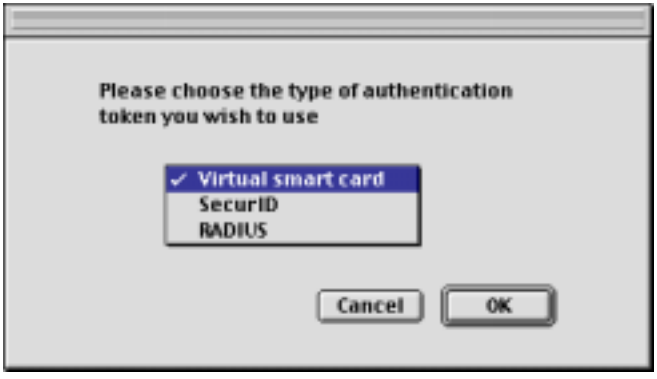
Depending on how the SmartGate administrator configured your version of SmartPass, you may need to enable your authentication token. SmartPass for Macintosh supports multiple tokens being enabled and running at the same time. Enable the authentication types you want by selecting **Preferences** and then **Use authenticator type...** under the **Edit** menu (Figure 6–2).

Figure 6–2
Edit/Preferences Menu



Select the type of authentication token you want to use from the Enable Authentication Token Dialog Box (Figure 6–3).

Figure 6–3
Enable Authentication Token Dialog Box



NOTE: A corresponding menu is added to the Menu Bar for each token type as they are enabled.

You must repeat this process for each additional token type you want enabled.

Using a Virtual Token

After launching SmartPass for the first time and enabling **Virtual smart card** in the Enable Authentication Token Dialog Box, you must create at least one virtual token.

Creating a Virtual Token

You can create a new token by selecting **Create virtual token...** from the **Virtual Token** menu (Figure 6–4).

Figure 6–4
Virtual Token Menu Bar

NOTE: This example menu bar displays all possible authentication token types as enabled.

The Create Virtual Token Dialog Box is displayed (Figure 6–5).

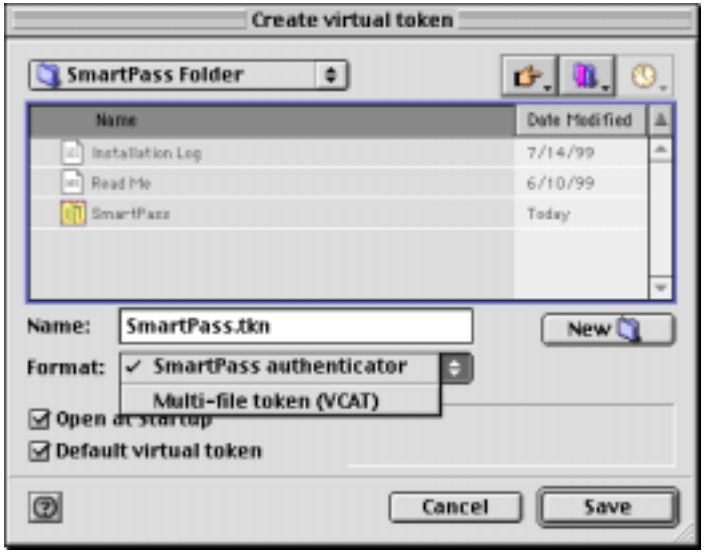


Figure 6–5
Create Virtual Token Dialog Box

NOTE: The "?" button launches Mac help.

If you are using multiple tokens, you may want to individualize the name appropriately, such as "yourname.tkn," which will appear as the title of the Access Code Prompt Dialog Box. You can also save it to a different location, such as your desktop. Click **Save** to complete. You will be prompted to create an Access Code for your new token.

Opening a Virtual Token

Open an existing token by selecting **Open virtual token...** from the **Virtual Token** menu. Figure 6–6 is displayed.

Figure 6–6
Open Virtual Token Dialog Box

Open at Startup – Select this check box if you want this token to be opened each time you run SmartPass. This option can be selected on multiple tokens.

Default virtual token – Select this check box if this token is the one in which new keys created during OLR should be stored.

Select the token you want to use and click **Open**. You will be prompted for your token's Access Code (Figure 5–7), chosen during the token's creation.

WARNING! You must enter an Access Code within 30 seconds from the time the Access Code Dialog Box is displayed, or the session will be canceled. The length of time the system will "remember" the Access Code is displayed in the **Keep** box. After that length of time, you will have to reenter your Access Code before performing a secure function. You may change this time limit by entering a new time (in minutes) in the **Keep** box. To disable this function, deselect the check box preceding **Keep**.

Figure 5–7
Access Code Prompt Dialog Box

If an incorrect Access Code is entered more than three consecutive times, SmartPass will be disabled and you must OLR again.

Performing On-Line Registration

SmartPass operates transparently. No proxy settings are necessary unless your network configuration requires that you use a Web proxy to navigate an intermediate firewall. If so, you should first establish that proxy setting as indicated in the "Configuration" section later in this chapter.

SmartPass uses a browser-based On-Line Registration (OLR) process. In order to perform OLR:

- Launch SmartPass.
- Open a Web browser.
- Enter the URL `http://your.smartgate.domain:3845/OLR` as the browser address or as instructed by your administrator.
- A Web OLR form will appear in the browser. Enter the required data and click **Register**.

After you have successfully registered, your authentication information will be saved in the default virtual token. If there is a problem with registration, an error message will appear in the Web browser.

NOTE: You do not perform OLR if you are using either SecurID or RADIUS authentication. Proceed to "Using SecurID Authentication" or "Using RADIUS Authentication" for more information.

NOTE: You don't need SmartPass to access the Web OLR form, but you must start SmartPass before clicking **Register**.

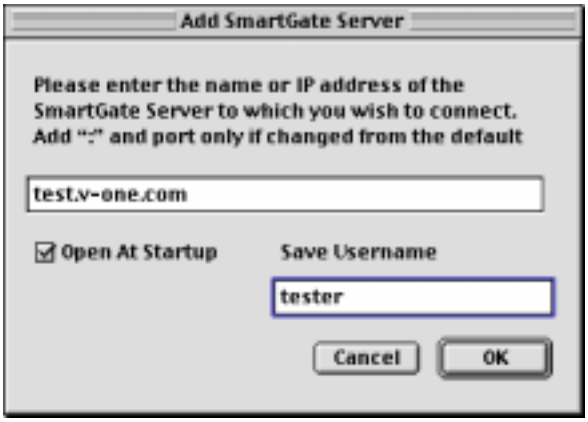
NOTE: The URL for the multiple port OLR Web page is `http://your.smartgate.domain:2090/30reg.html`.

Using RSA SecurID Authentication

NOTE: Each token type must be enabled in order for it to be displayed on the menu bar.

After launching SmartPass for the first time and enabling **SecurID** in the Enable Authentication Token Dialog Box, you will need to specify at least one SmartGate Server. Do this by selecting **Add Server...** from the **SecurID** menu. The Add SmartGate Server Dialog Box (Figure 5–8) is displayed.

Figure 5–8
Add SmartGate Server Dialog Box



NOTE: Additional servers may be added by repeating this process.

Enter the hostname or IP address of the SmartGate/SecurID Server being used.

The SmartGate Server's default SecurID port is 2095. If the TCP port was changed in the startup daemon, append a colon "**:**" and the port number to the server's name or address.

Open at Startup – Select this check box if you want this server to be opened each time you run SmartPass. This option can be selected for multiple servers.

Save Username – If **Open at Startup** is selected you have the option to save the username assigned to you by your network administrator. During startup, the SecurID Login Dialog Box will reflect this information.

After adding a SmartGate/SecurID Server, the SecurID Login Dialog Box (Figure 5–9) will prompt you for your **Username** and **Passcode**.

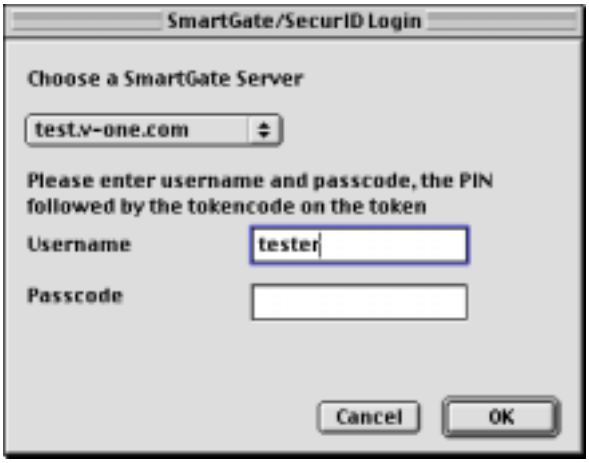


Figure 5–9
SecurID Login Dialog Box

NOTE: The SecurID Login Dialog Box is presented every time SmartPass is launched and each time an authentication has timed out.

Enter the Username that identifies you as a user to RSA's ACE/Server. Enter the Passcode, which is a combination of an assigned PIN code and the token code displayed on the RSA SecurID token. The token code is regenerated at timed intervals. SmartPass sends this user information to the SmartGate/SecurID Server, which relays it to the ACE/Server. RSA's username and passcode will have been provided to you by your network administrator.

NOTE: The **Passcode** must be a minimum of 6 characters and a maximum of 16 characters.

The ACE/Server performs all RSA SecurID authentications relaying one of three possible responses back to SmartPass via the SmartGate/SecurID Server:

1. **Success**—The user, identified by his username and passcode, has been authenticated.
2. **Next Code**—The user must submit the next token code from the token's display. A dialog box similar to the SecurID Login Dialog Box will be displayed, except that the user is only prompted for the next **Tokencode** rather than a **Username** and full **Passcode**.
3. **New PIN**—The user must create a new PIN. There are 3 forms of this response: the user must create his own PIN, accept the server generated PIN, or choose between creating a personalized PIN or using the server generated one. Use the displayed dialog box to enter or accept your new PIN.

WARNING! The **Next Code** response must be the token code immediately following the token code submitted in the initial login dialog.

Communication between SmartPass and the SmartGate/SecurID Server is encrypted using standard SmartGate security mechanisms.

Using RADIUS Authentication

NOTE: Each token type must be enabled in order for it to be displayed on the menu bar.

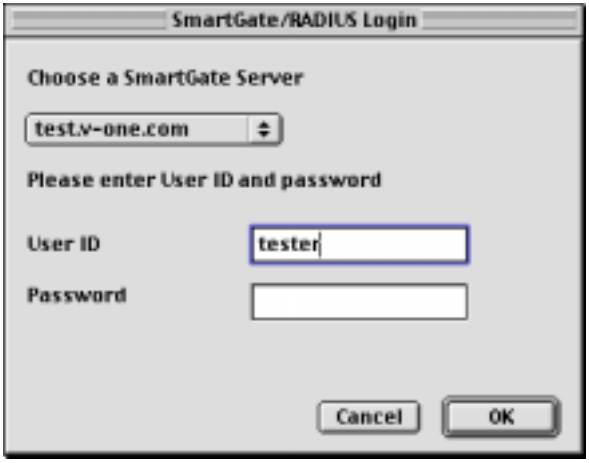
After launching SmartPass for the first time and enabling **RADIUS** in the Enable Authentication Token Dialog Box, you will need to specify at least one SmartGate/RADIUS Server. Do this by selecting **Add Server...** from the **RADIUS** menu. The Add SmartGate Server Dialog Box (Figure 5–10) is displayed.

Figure 5–10
Add SmartGate Server Dialog Box

NOTE: Additional servers may be added by repeating this process.

After adding a SmartGate/RADIUS Server, the RADIUS Login Dialog Box (Figure 5–11) will prompt you for your **User ID** and **Password**.

Figure 5–11
RADIUS Login Dialog Box



Enter the administrator-provided User ID and password that identify you as a user to the RADIUS Backend Server. The RADIUS Backend Server performs all RADIUS authentications

by relaying one of three possible responses back to SmartPass via the SmartGate/RADIUS Server:

1. **Success**—The user, identified by their User ID and password, has been authenticated. The SmartGate administrator sets how long each SmartGate session lasts before a new authentication is required.
2. **Failed**—The user has failed to be authenticated. A text message from the server will explain why authorization failed.
3. **Challenge**—The SmartGate/RADIUS Server received a Challenge/Response request from the RADIUS Backend Server. The user must respond to the challenge(s) before they can be authenticated. Challenge/Response is a product of specific programing by the SmartGate administrator and consequently may not be used.

Communication between SmartPass and the SmartGate/RADIUS Server is encrypted using standard SmartGate security mechanisms.

Running Secure Applications

To run secure applications, you must:

- Ensure that the IP connection is active.
  - If you are using a dial-up connection, dial the service provider and log on.
  - If you are connected to a LAN, make sure that its normal (unsecured) services can be accessed.
- Start SmartPass and enter your Access Code.

NOTE: This section assumes that you have already installed SmartPass, enabled your tokens, and either registered or added a SmartGate Server, depending on your token.

Configuration

If there is a firewall between your client station and the SmartGate Server, you may need to configure SmartPass to successfully negotiate that firewall using a proxy. Consult with your system/network administrator for specifics on your firewall situation.

Using a Web Proxy to Navigate a Firewall

You can connect to both secure and non-secure Web sites using a Web (HTTP) Proxy. In addition, the SmartPass Single Port Proxy operation allows for secure connections for generic TCP applications, such as, FTP, Telnet, and e-mail, using a Web Proxy.

If your network configuration requires that you use a local proxy for Web access, you should specify this using `InternetConfig` or the `Internet` Control Panel in MacOS 8.5. `InternetConfig` and `Internet` are just different user interfaces for setting the same preferences, so you may use whichever you prefer.

There is no additional configuration necessary for firewalls that require a username/password authentication. SmartPass automatically prompts for your firewall's username and password, and then maintains it for the duration of that SmartPass session. You must obtain your firewall's username/password from your network administrator.

Configure Using `InternetConfig`

`InternetConfig` is distributed with many applications and is also available from many download sites.

Using `InternetConfig`, go to the **Firewalls** panel, select the **Use HTTP Proxy** check box, and specify the address of the proxy in the form ***host*:*port***, (for example: **123.45.67.89:80**). Also, you must specify **127.0.0.1** (localhost) in the **No Proxy for** field in order for On-Line Registration to function correctly.

Microsoft Explorer uses `InternetConfig's` settings. However, if you are using Netscape, you must, in addition to `InternetConfig`, specify the proxy settings to Navigator/Communicator using the **Edit** menu. Select **Preferences**, **Advanced**, and **Proxies**; and then enter the address and port of the proxy.

Configure Using Internet Control Panel

The Internet Control Panel is part of MacOS 8.5 and later.

From the **Edit** menu, select **User Mode...** and then **Advanced**. Select **Firewalls** from the **Preferences** menu, or click the **Advanced** tab and scroll to the **Firewalls** icon. Select the **Web Proxy** check box and specify the address and port of the proxy. Also, you must specify **127.0.0.1** (localhost) in the **Bypass proxies for these hosts** field in order for On-Line Registration to function correctly.

Microsoft Explorer uses Internet's settings. However, if you are using Netscape, you must, in addition to Internet, specify the proxy settings to Navigator/Communicator using the **Edit** menu. Select **Preferences**, **Advanced**, and **Proxies**; and then enter the address and port of the proxy.

Using an SSL Proxy

You can create secure connections for generic TCP applications, such as, FTP, Telnet, and e-mail, using an SSL Proxy, which will operate in tunneling mode. You can also connect to secure Web sites using an SSL Proxy if a Web Proxy is not being used.

From the **Edit** menu, select **Preferences** and then **Use SSL Proxy**. The SSL Proxy Dialog Box is displayed (Figure 5–12).

Figure 5–12
SSL Proxy Dialog Box

NOTE: If SmartPass is running in Single Port mode, all connections can be made using the Web Proxy.

Enter the hostname or IP address of the SSL proxy being used. The default port is 443; append a colon **":"** and the port number to the host's address if it is different.

Select the **Use Authentication** check box if you are transversing a firewall that requires username/password authentication. The **Username** and **Password** fields are displayed only if **Use Authentication** is selected.

SmartPass File Location Information

SmartPass is a standard Macintosh application requiring two extensions in the `Extensions` folder of your `System` folder, however, there are no SmartPass components in the `Control Panels` folder for startup, configuration, or other operations.

SmartPass looks first for its preferences file, `SmartPass Preferences`, in the same folder as the application. If not found, it looks in the folder `V-ONE Data` in the `Preferences` folder of the startup disk, creating them if necessary. A virtual token may also be stored in this folder.

Multiple User Support

SmartPass supports a number of different configurations for multiple users who may share one computer. Each user should copy the file `SmartPass Preferences` to a suitable location, changing the name as appropriate and customizing the preferences as desired. Double-clicking the file icon starts SmartPass using that set of preferences. You may rename a FIPS token file name (i.e., `yourname.tkn`) or a `VCAT` folder, however, you cannot change the names of the files within the folder.

Performing Other System Functions

There are several other functions that you may want to perform, such as:

- Backing up your virtual token
- Changing your virtual token's location
- Uninstalling SmartPass
- Adding or changing your authentication key (virtual tokens only)

Backing Up Your Virtual Token

To back up a virtual token to a floppy disk or other media, simply copy the file (example, `yourname.tkn`) or, in the case of a VCAT, the entire folder to the disk. When a VCAT is being used, the folder is usually named `VCAT` and usually resides in the `V-ONE Data` folder.

Changing Your Virtual Token's Location

To change a token location:

1. Move the file (example, "`yourname.tkn`") or, in the case of a VCAT, the folder (example, "`VCAT`") to the new destination.
2. When you start SmartPass, select **Preferences** and then **Delete Startup Items** from the **Edit** menu. This will tell SmartPass to forget the token's old location.
3. Specify the virtual token's new location by using the Open Virtual Token Dialog Box (see Figure 6–6).

Uninstalling SmartPass

To uninstall SmartPass:

1. Drag the folder into which you installed the software (default is `SmartPass Folder`) to the Trash.
2. You should also trash the `SmartPass Module` in the `Extensions` folder.

You can delete virtual tokens in the same way.

Adding or Changing Your Authentication Key

NOTE: This function is only used for virtual tokens (example, FIPS or VCAT).

To add or change your authentication key:

1. Run the **Smartcat Utility** which is downloaded with the SmartPass software.
2. Open the virtual token that you want to edit; a list of keys will be displayed.
3. Double-click the key you want to modify.
4. The Edit User Window appears and displays:

   User Name
   Keyname
   Key ( )
   Hostname

NOTE: The original key is blanked with '*'s.

5. Enter a new key value

Changing the Default Single Port Proxy on SmartPass for the Macintosh

Communication between SmartPass for the Macintosh and the SmartGate Server uses the Single Port Proxy, defaulted at 3845. Changing the default is **not** recommended. If you **must** change the default Single Port Proxy, both the SmartGate Server and the SmartPass software need to be configured.

NOTE: The Mac Client will try to connect to the SmartGate Server on 3845, 443, and 80.

As SmartGate administrator, you can configure the SmartGate Server accordingly. However, you will need to contact V-ONE Technical Support at (800) 495–VONE (8663) or customercare@v-one.com regarding changing the Single Port Proxy default in SmartPass for the Macintosh.

For instructions on changing the default Single Port Proxy from 3845 on either a Windows NT or UNIX-based SmartGate Server, see "Changing the Default Single Port Proxy" in Chapter 5, "Using SmartAdmin," in the *SmartGate Administrator's Guide*.

Glossary

3DES: *See* "Triple DES Encryption"

Access Code: The secret code, similar to a PIN on an ATM card—required to unlock the authentication key stored on the user's token each time the user accesses a secure service. This code, defined by the user during registration, must be at least four characters in length with a maximum of 16, and can be any combination of letters and numbers.

The length of time the system will 'remember' the Access Code is displayed in the **Remember code for: *xxx* minutes** field in the Access Code Dialog Box. The default limit is 10 minutes, however, the user may change the time limit by entering a new time (number of minutes—maximum of 999). SmartPass resets the limit every time Dynamic Configuration is performed.

Access Control: Allowing or denying connections through the use of access permissions.

Access Permissions: The associations between users and connections, as defined by a User ID, group name, service (TCP or Web), or destination. SmartGate access permissions can be either individual user permissions or group permissions.

Authentication: The process of determining the identity of a user attempting to access a system.

Authentication Key: The key is a 32-character hexadecimal key assigned to a user during installation by the registration server administrator, consisting of the numbers 0 to 9 and letters A to F.

The SmartGate authentication system supports virtual smart cards and ISO-standard smart cards for both authentication and stored data. A user with a physical smart card must use a smart card reader connected to their PC. Virtual smart card information (VCAT token) may be stored on either the PC hard drive or a removable (floppy) disk.

The user's SmartGate authentication key is stored on the smart card, whether physical or virtual. This information is shared with the SmartGate Server, where it is stored in the SmartGate Server's user database.

Authentication Token: A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.

Authenticator: The name assigned to a SmartGate Server through which users can access a particular service. This name can be up to 14 alphanumeric characters in length and it is recommended that it be a derivative of your SmartGate Server hostname.

Challenge/Response: An authentication technique whereby a server sends an unpredictable challenge to the user. The user then computes a response using some form of authentication token.

CHIPDRIVE external Smart Card Reader: A device, developed by TOWITOKO electronics, used to read the information contained on a physical smart card. The CHIPDRIVE external card reader plugs directly into the serial port and does not need a battery.

Client Port: The TCP/UDP port number your application will use to gain access to the secured services on a TCP/IP network. this is used when you want to make connections via localhost rather than the Winsock shim and is configured by the SmartGate administrator in the access control list.

For Example:

21	Used for FTP
2023	Used for Telnet
25	Used for SMTP (example, sendmail services)
110	Used to retrieve messages using POP3 mail protocol

Client/Server: Computer technology that separates computers and their users into two categories: clients or servers. When you request information from a computer, you are a client. The computer that provides the information is the server. A server both stores information and makes it available to any authorized client who requests the information.

Digital Certificate: A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticated users can look up other users' public keys.

DES Encryption: Data Encryption Standard. A U.S. government-approved method of encryption that currently uses a 56-bit key.

DNS: See "Domain Name Service."

Domain Name: Identifies a 'location' on the Internet (example, v-one.com) that has been registered with the Internet Network Information Center (InterNIC). Currently the domain name is limited to 47 characters. Through the use of aliases, however, it is possible to accommodate longer names. You may contact V-ONE Corporation for support in this connection.

Domain Name Service (DNS): The distributed database that maps Internet domain names to IP addresses or IP addresses to Internet domain names, in addition to containing other information.

End User: Those users who connect to a SmartGate Server using the SmartPass client software on their personal computers.

Entrust Authentication: The Entrust authentication method allows SmartPass users to use an Entrust soft token as an alternative authentication method. Entrust provides digital certificates to create an on-line identification and security system for the Internet. Both SmartPass and the SmartGate/Entrust Server must obtain their credentials from the Entrust CA Server, enabling both sides to validate the other party during the authentication process.

Entrust Certification Authority (CA) Server: The Entrust Server representing the organization or group of people who are responsible for setting security policies regarding the protection of sensitive and valuable data and assigning secure electronic identities in the form of certificates. These people are referred to collectively as the Certification Authority (CA).

Entrust/Netrust Authorization code: The Authorization code issued by the Entrust or Netrust CA Server.

Entrust/Netrust Directory: The directory where your Entrust or Netrust files (specifically `entrust.ini` and, when using UNIX, the run-time library files) are installed. The `entrust.ini` file contains the location of the Entrust or Netrust CA Server and Manager and is used by both the SmartGate Server and SmartPass. The `entrust.ini` file is obtained from Entrust or Netrust—not V-ONE—It is necessary for the operation of the software.

Entrust/Netrust Reference Number: The Reference number issued by the Entrust or Netrust CA Server.

FIPS 140-1: Compliance with FIPS 140-1 government coding standards.

FIPS Token: A software emulation of a hardware authentication token that is in compliance with the FIPS 140–1 coding standards. It stores your private information (authentication key) in an encrypted file system, either on a floppy disk or on your hard drive.

Firewall: A system or combination of systems that enforces network access policies between two or more networks.

Firewall Host Name (or IP Address): This is either a valid DNS name or an actual IP Address (example, `206.133.19.26`) used to connect to a SmartGate Server.

Firewall Port: This is the TCP/IP port number the SmartGate Server will be listening on for secure connection requests by SmartPass (example, 2023, 2021). This port will be assigned by the SmartGate Server administrator.

Firewall-to-Firewall Encryption: All traffic from one firewall to another over the Internet is automatically encrypted.

Format Smart Card: This function erases the current secret format code from a smart card, and returns it to the default secret code. The authentication key is **NOT** removed during the formatting process.

Format Code: A 4- to 16-character code which allows the user to format a smart card.

FQDN: Fully Qualified Domain Name. This is a hostname which will include the hostname and domain name. For example, the machine "test" within the domain "`v-one.com`"—it's FQDN would be "`test.v-one.com`".

FTP: FTP (File Transfer Protocol) is a way of moving one or more files from one computer to another on the same network. It is especially useful when the files are too large to fit on a floppy disk and when moving files between different operating systems.

G&D STARCOS Smart Card: A microprocessor-based physical smart card manufactured by Giesecke & Devrient GmbH (G&D).

Gemplus MCOS Smart Card: A microprocessor-based physical smart card manufactured by Gemplus.

Integrity: The assurance that any data has not been altered in transmission.

IP: Internet Protocol.

IP Payload Compression (IPCOMP)—IPSec: A method of compressing the data in the payload of an IP packet so that it will take up less bits on the wire. V-ONE supports the DEFLATE protocol.

IPSec: Internet Protocol Security (IPSec). A suite of protocols used for secure private communications over the Internet. The proposed suite of IPSec protocols would create a standard platform for securing IP connections on private networks. These protocols basically deal with authentication, encryption, and key management.

ISA: Industry Standard Architecture. An expansion bus commonly used in PCs, it accepts plug-in boards currently being superceded by "PCI" boards.

Key: *See* "Authentication Key"

Linux: Linux is a UNIX operating system clone which runs on a variety of platforms, especially personal computers with Intel 80386 or better processors. It supports a wide range of software, from TeX, to the X Window System, to the GNU C/C++ compiler, to TCP/IP. It is a versatile, bona fide implementation of UNIX, freely distributed under the terms of the GNU General Public License.

Logging: The process of storing information about events that occurred on the firewall or network.

Log Retention: How long audit logs are retained and maintained.

Log Processing: How audit logs are processed, searched for key events, or summarized.

MCOS: *See* "Gemplus MCOS smart card"

Mutual Authentication: Bidirectional authentication where the client is required to authenticate to the server, and the server is required to authenticate to the client.

Netrust Anonymous Registration: Anonymous registration allows a Netrust end user to log in and register to the SmartGate/Netrust Server without performing OLR. When a user is registered anonymously, they are identified in the SmartGate user database by an ID derived from their Netrust smart card's serial number, which displays as a random string of numbers.

Netrust Authentication: The Netrust authentication method allows SmartPass users to use a Netrust ready smart card and smart card reader instead of other V-ONE tokens, such as a VCAT token. Both SmartPass and the SmartGate/Netrust Server obtain their credentials from the Netrust Certificate Authority (CA) Server. Both sides will validate the other party during the authentication process. See *Using SmartGate With Netrust Authentication* for complete information on Netrust.

Netrust Certification Authority (CA) Server: The Netrust Server representing the organization or group of people who are responsible for setting security policies regarding the protection of sensitive and valuable data and assigning secure electronic identities in the form of certificates. These people are referred to collectively as the Certification Authority (CA).

Network Adaptor Card: A card that connects a terminal device to the network.

Non-repudiation: Ensuring that the original message has not been altered since it was sent.

On-Line Registration (OLR): All SmartPass end users must register before they can access the system. OLR provides a means by which users can register at their computer, immediately after installing the SmartPass software.

Password: A sequence of characters which, when combined with a user name, limits a logon only to the authorized user.

PCAT Parallel Smart Card Reader: A device used to read the information contained on a physical smart card.

Physical Smart Card: Credit card-sized device implanted with integrated circuit chips used for a variety of applications, such as financial debt/credit transactions and computer security. *See also* "Smart Card Technology"

Privacy: The authorized distribution of information (who has a right to know what).

Private Key Cryptography: An encryption method which requires both parties of a digital transmission to know the same key for encryption and decryption.

Proxy: A software agent that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, may perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

Public Key Cryptography: An encryption method that allows secure communication between two parties who have not transmitted a private key in advance. Each party transmits a public

key used to encode messages to itself. Public key messages can only be decoded with a private key which is never transmitted.

RADIUS Authentication: RADIUS authentication is an open-standard (RFC 2138) authentication protocol transported over UDP, not TCP.

Remote Authentication Dial-In User Service (RADIUS): An authentication method using a username/password combination with MD5 hashing of password for increased security. Described in RFC 2138.

Remote Host Name: Either a valid DNS name or an actual IP Address (example, `206.133.19.26`) that identifies the host on which the secured service is provided. A SmartGate Server will connect to this host after SmartPass completes an authenticated session connection. You will be given the correct value to use for each designated service by your SmartGate Server administrator.

Remote Host Service Port: This is the port number the designated remote service host will be listening on to accept connections for service from a SmartGate Server after any user is successfully authenticated for service.

RSA SecurID Authentication: A dual-factor authentication method using the SecurID token and ACE/Server authentication products developed by Security Dynamics, Inc. (SDI). SmartGate supports all types of SecurID authentication tokens, including the standard card/key fob, PINPAD card, and SoftID card.

Rule Set: The group of instructions that determine distribution of system privileges to users.

SCSI (Small Computer System Interface): Pronounced "scuzzy," SCSI is a hardware interface that allows for the connection of up to seven peripheral devices (hard disk, CD-ROM, scanner, etc.) to a single expansion board in a computer.

Security: Protection or defense against unauthorized access to data. The four attributes of security are: Authentication, Integrity, Privacy, and Non-repudiation.

Server: *See* "Client/Server" or "SmartGate Server"

Single Port Proxy: The SmartGate Single Port Proxy provides the various SmartGate services with a single-port presence on the perimeter of a network. Therefore, all SmartPass to SmartGate connectivity will pass through the Single Port Proxy and be forwarded to the correct destination SmartGate service. The Single Port Proxy is defaulted at 3845, and can be changed with the "deployability" option.

Smart Card: *See* "Physical Smart Card" *or* "Virtual Smart Card"

Smart Card Reader: A device used to read the information contained on a physical smart card. At present, SmartPass supports V-ONE's PCAT parallel smart card reader, Fischer's Smarty reader, and TOWITOKO electronics' CHIPDRIVE external card reader.

Smart Card Technology: Credit card-sized device implanted with integrated circuit chips used for a variety of applications, such as financial debt/credit transactions and computer security, a device to read the information contained on the card, and software controls.

SmartAdmin: SmartGate's stand-alone administrative software, which is used to manage user information and access permissions, including administrative rights. Using SmartAdmin, a SmartGate administrator may also configure the SmartGate Server and its Single Port proxy mapping rules. SmartAdmin runs remotely on a Windows 95 or 98 and either remotely or locally on a Windows NT Server.

SmartGate Group: Users grouped by organization, such as department (example, accounting or sales), location (example, Chicago), or artificial community, such as a project being managed as an independent set of services (example, ProjectX). A SmartPass end user belongs directly to one SmartGate group. However, in addition to the group "all," the user can be given the permissions of as many groups as desired. The group's name can be up to 23 characters in length and cannot include spaces or special characters.

SmartGate Hostname or IP Address: Either a valid DNS name or an actual IP address (example, `206.133.19.26`) used to connect to a SmartGate Server.

SmartGate Port: This is the TCP/IP port number the SmartGate Server will be listening on for secure connection requests by SmartPass (i.e., 2023, 2021).

SmartGate Server: The machine running the SmartGate Server software. Logically, this is the machine between the user's personal computer and the ultimate destination for the application being secured by SmartGate.

SmartGate Server Administrator: The person responsible for maintaining the SmartGate Server and user authentication database on the SmartGate Server.

SmartGate Web Group: A group of SmartGate users or groups requiring access to the same remote host services.

NOTE: This applies only to Web services which may be accessed through the SmartGate Server.

SmartPass: The client software that runs on the end user's personal computer and is used to connect to the SmartGate Server.

Smarty Reader: A device, developed by Fischer International, used to read the information contained on a physical smart card. The Smarty reader simulates a 3.5-inch computer disk. The physical smart card is inserted into the Smarty reader which, in turn, is inserted into the computer's floppy drive.

SMTP: Simple Mail Transfer Protocol.

Soft Token: *See* "FIPS Token" *or* "VCAT Token"

STARCOS: *See* "G&D STARCOS Smart Card"

TCP/IP (Transmission Control Protocol/Internet Protocol): This is the suite of protocols that defines the Internet.

Telnet: An Internet protocol and program that enables you to connect your PC as a remote workstation to a host computer, and to use that computer as if you were logged on locally.

Triple DES Encryption (3DES): A method of encryption that uses a 168-bit key. There are four separate situations in which 3DES encryption is an option; SmartGate protocol packets used to manage client/server secure communications, proxy data packets used to convey end user data between client and Server, and internal server communication between the Authentication Server and the proxy. 3DES is also an option when configuring specific IPSec channel types.

Uniform Resource Locator (URL): The server and path information used to specify the location of a document. Formatted as follows:

```
scheme://host-domain[:port]/path/filename
```

The maximum length allowed for a URL in SmartPass is 256 characters.

User ID: The identification associated with the authentication key which is either generated during OLR or assigned by the SmartGate Server administrator when the user is added to the SmartGate Server database. A User ID may be up to 30 characters in length and cannot include spaces or special characters. However, your User ID defaults to the authentication token manufacturer's parameters. For example, the MCOS and STARCOS physical smart cards have a limit of 15 characters for the User ID. Each User ID must be unique on the SmartGate Server where it resides.

User Name: *See "User ID"*

VCAT Token: A software emulation of a hardware authentication token. It stores your private information (authentication key) in an encrypted file system, either on a floppy disk or on your hard drive.

Virtual Private Network (VPN): A private network created over a public network (example, the Internet) by using encryption, where exclusive client and host communications can occur.

Virtual Smart Card: *See "FIPS Token" or "VCAT Token"*

World Wide Web: Generally used to refer to the whole constellation of Internet resources that can be accessed using Gopher, FTP, HTTP, Telnet, USENET, WAIS and other tools. Also, the universe of hypertext (HTTP) servers that allow text, graphics, sound files, etc., to be mixed and accessed.

Appendix A

SmartPass Files

This appendix contains detailed descriptions of the SmartPass files that you should customize to reflect your organization's requirements. As the SmartGate administrator, you should configure SmartPass prior to deploying the software to your end users. Following the file descriptions are explanations of each of the configuration options available for the SmartPass configuration file, `setup.ini`. These options include the different available authentication tokens and readers, On-Line Registration (OLR) launching capabilities, installation splash screen branding, and desktop icon labeling.

Detailed Description of `setup.ini`

SmartPass Configuration File

Used By: The SmartGate administrator to configure installation values in the SmartPass software prior to distribution to end users.

Purpose: By configuring the `setup.ini` file, the SmartGate administrator has the ability to limit the installation package to specific authentication tokens and readers and configure the installation to search and remove SmartPass 2.2.*x* files. The administrator may also set up the end user's On-Line Registration (OLR) with certain launching capabilities and desktop icon labeling.

Location: SmartPass installation disk.

Structure: This file consists of comment lines and control lines. The length of each line is limited to 255 characters including spaces. Comments must be preceded by a semicolon (;). Each control line is a *name=value* pair. Name is not case sensitive.

Customization: This is a text file that you can edit using a simple text editor, such as Notepad.

Option Descriptions of `setup.ini`

This section contains descriptions of the configurable options in the SmartPass configuration file, `setup.ini`.

Labeling Installation Splash Screen

AppName

Purpose: Specifies the banner title located at the top of the SmartPass installation splash screens.

Format: AppName=*text*

Value(s): *text* is the title of the SmartPass installation screens.

Default: `SmartPass 4.1`

Example: `AppName=SmartPass 4.1 Installation`

Installation Packaging

Packages

Purpose: Specifies the type(s) of authentication your users will be using to create secure paths to the SmartGate Server. Configure this setting with the authentication tokens to be used by your end user population.

Format: Packages=*option1,option2,...*

Value(s): *option1,...* are the optional packages that can be included in the SmartPass installation package. They are:

FIPSTOKN	-	FIPS 140–1 compliant virtual authentication token
VCAT	-	Virtual smart card emulation
STARCOS	-	G&D STARCOS smart card
MCOS	-	Gemplus MCOS smart card
PCAT	-	V-ONE's smart card reader
SMARTY	-	Fischer's Smarty card reader
CHIPDRV	-	TOWITOKO's CHIPDRIVE external smart card reader
CARDFMT	-	Smart card formatting program for either PCAT, CHIPDRIVE, or Smarty card readers
SGSDI	-	RSA SecurID authentication
RADIUS	-	RADIUS authentication
SGENTRUS	-	Entrust authentication
ENTRUST	-	Entrust authentication (files must be obtained from Entrust)

NOTE: The order of the options does not matter.

NOTE: If both a VCAT and a FIPS token are installed during a new installation, the FIPS token becomes the default. If, however, the user is upgrading with an existing VCAT, the VCAT remains the default. The user can, of course, change which token is used.

SGNETRUS	-	Netrust authentication
NETRUST	-	Netrust authentication (files must be obtained from Netrust)
SHIM	-	Winsock call interception shim
IPSEC	-	IPSEC network level security
BROWSER	-	This package, which is never required and is not needed when installing the shim package, can be installed to make SmartPass change the browser proxy settings on startup. This functionality used to be in the base product but now is an optional component.
PKI	-	PKI authentication

Default: FIPSTOKN,MCOS,SHIM,VCAT

Example: `Packages=FIPS,MCOS,SHIM,IPSEC`

OLR Launching Options

The SmartGate administrator may configure the SmartPass installation disk to automatically launch the user into a specified URL address (example, the company OLR page) and/or a specified program following installation and launching of the SmartPass software. The three configuration options are:

- `OLRPage`
- `Execute`
- `ExecutePrompt`

Detailed descriptions follow.

OLRPage

Purpose: Specifies the On-Line Registration URL, such as the standard single port OLR Web page (`http://your.smartgate.domain:3845/OLR`) or your manually created OLR Web page, which will be used to perform OLR. This entry will be used to create an icon and a program menu choice entitled **On-Line Registration**.

Format: OLRPage=*URL:port/OLRform*

WARNING! If you are using the HTTP (Web or SSL tunneling) Proxy with authorization required, do not use the `OLRPage` option in the `setup.ini` file.

Value(s): *URL* is the OLR Web page to be accessed to perform On-Line Registration.

port is the port number that the SmartGate OLR Server will listen on.

OLRform is the name of the HTML OLR form generated on-the-fly from the OLR field descriptions and branding options configured on the SmartGate Server.

Default: None.

Example:

`OLRPage=http://www.v-one.com:3845/OLR` (single port)
`OLRPage=http://your.smargate.server:2090/30reg.html` (multiple port)

NOTE: The SmartGate administrator can create a custom OLR Web page and point her users to this site. See "Manual Setup of an HTML Page for On-Line Registration" in Chapter 7, "On-Line Registration Services," in the *SmartGate Administrator's Guide*, for more information.

Execute

Purpose: Specifies what program to execute immediately following installation of the SmartPass 4.*x* software.

Format: Execute=*program arguments*

Value(s): *program* is the program or programs to be executed.

arguments is used when the program requires further parameters, such as a Web URL to be opened.

Default: None.

Example: The following will cause the OLR process to be invoked:

`Execute=vspstart -h http://www.v-one.com:3845/OLR`

The following will cause the smart card formatting utility to be invoked and on completion of that utility, OLR to be invoked:

`Execute=card_format /d vspstart -h http://www.v-one.com:3845/OLR`

NOTE: This option is **only** invoked after installation.

NOTE: OLR will not be automatically launched after setup unless the Execute entry is completed.

ExecutePrompt

Purpose: Specifies the text that is displayed in the message prompt that follows installation. There are two options available depending on installation configuration.

If the computer needs to restart, the message prompt will be:

`Would you like to automatically run the ... following the restart of this computer?`

If the restart is not necessary, the message prompt will be:

```
Would you like to run ... now?
```

Format: ExecutePrompt=*prompt*

Value(s): *prompt* is the text that will be displayed in the user prompt.

Default: None.

Example:

```
ExecutePrompt=SmartPass On-Line Registration
```

PortList

Purpose: This entry configures which ports, in order, SmartPass will try to navigate through a firewall to initiate a secure session to the SmartGate Server.

WARNING! Do NOT use port 443 or 80 if either an SSL Server or a Web Server, respecively, is running on your SmartGate Server.

Default: 3845,443,80

Valid Range: A comma deliminated list of integer values between 1 and 65536

Example: 3845,443,80,6830

Detection Options

Remove22x

Purpose: Detects and removes any SmartPass 2.2.*x* programs as part of the installation procedure.

WARNING! Any existing SmartPass 2.2.*x* VCATs are also removed.

Format: Remove22x=*yes*

Value(s): *yes* SmartPass 2.2.*x* products are searched for and removed during installation.

Default: None.

Example: `Remove22x=yes`

DetectCardRemovalInterval

Purpose: Detects the removal or change of a user's smart card. Periodically, SmartPass verifies that the smart card is still inserted into the smart card reader and that the serial number of the smart card is the same as the smart card that logged on.

Format: DetectCardRemovalInterval=*# of seconds between polling intervals*

Value(s): 10 to 3600 seconds

Default: Off.

Example: `DetectCardRemovalInterval=30`

Winsock Shim Warning Messages

WSOCK32WARN*x*

Purpose: Configures the installation program message that will display if the WSOCK32.DLL currently in the Windows system directory is from a vendor other than V-ONE or Microsoft.

Format: **WSOCK32WARN*x*=*text***

Value(s): *x* A number 1 through 4.

text The text that will be displayed in the warning message.

Default: None.

Example:

```
WSOCK32WARN1=Warning - A non-standard system compo-
nent (WSOCK32.DLL) is currently installed on this
machine.

WSOCK32WARN2=Continuing with this installation may
cause some installed programs not to work properly.
```

IPSec WINS Server Setup

These two IPSec-related options can be used to automatically set an end user's WINS Server address during installation of SmartPass. These options will automatically overwrite the user's WINS Server address. Consequently, they should be set only if you have a full understanding of your end user's environment, such as, if you are deploying SmartPass to company employees. Whereas, if you are deploying SmartPass to a partner company, so that they may access certain applications within your network, you would not want to set these options.

PrimaryWINSServer

Purpose: Configures the installation program to set the primary WINS Server to a specified IP address. This option is only available when the IPSEC package is installed.

Format: **PrimaryWINSServer=*IP address***

Value(s): *IP address* The IP address of the primary WINS Server.

Default: None.

Example: `PrimaryWINSServer=10.0.0.222`

SecondaryWINSServer

Purpose: Configures the installation program to set the secondary WINS Server to a specified IP address. This option is only available when the IPSEC package is installed.

Format: **SecondaryWINSServer=*IP address***

Value(s): *IP address* The IP address of the secondary WINS Server.

Default: None.

Example: `SecondaryWINSServer=10.0.0.223`

setup.ini

```
[Startup]
AppName=SmartPass 4.1
FreeDiskSpace=225
16on16=N

[V-ONE]
;OLRPage=
; Purpose:   This entry specifies the On-Line Registration URL to be
;            accessed to perform On-Line Registration.
; Default:   No default
; Example:   OLRPage=http://www.v-one.com:3845/OLR
; Notes:     This entry will be used to create a menu choice for On-Line
;            Registration under Programs in the user's Start Menu.
;
Packages=FIPSTOKN,MCOS,SHIM,VCAT
; Purpose:   This entry controls which of the optional packages on the
;            install disk are automatically installed.
;
; Default:   FIPSTOKN,MCOS,SHIM,VCAT
;
; Alternate packaging:
;            for SecurID authentication       - Packages=SGSDI
;            for RADIUS authentication        - Packages=RADIUS
;            for ENTRUST authentication       - Packages=SGENTRUS,ENTRUST
;            for NETRUST authentication       - Packages=SGNETRUS,NETRUST
;            for VCAT token user authentication- Packages=VCAT,MCOS
;            for IPSec level security         - Packages=FIPS,MCOS,IPSEC
; Example:   Packages=SMARTY,MCOS,SHIM,CARDFMT
;
; Notes:     Currently, the optional packages are:
;            FIPSTOKN  - FIPS 140-1 compliant virtual authentication token
;            VCAT      - Virtual smart card emulation
;            STARCOS   - G&D STARCOS smart card
;            MCOS      - MCOS smart card
;            PCAT      - V-ONE's smart card reader
;            SMARTY    - Fischer's Smarty card reader
;            CHIPDRV   - TOWITOKO's CHIPDRIVE extern smart card reader
;            CARDFMT   - Smart card formatting program for either
;                        PCAT, CHIPDRIVE, or Smarty card reader
;            SGSDI     - SDI's SecurID authentication
;            RADIUS    - RADIUS authentication
;            SGENTRUS  - Entrust authentication
;            ENTRUST   - Entrust authentication (files must be supplied by Entrust
;                        and copied to the install disk by administrator)
;            SGNETRUS  - Netrust authentication
;            NETRUST   - Netrust authentication (files must be supplied by Netrust
;                        and copied to the install disk by administrator)
;            SHIM      - WSOCK32.DLL call interception shim
;            IPSEC     - IPSEC network level security
;            BROWSER   - This package, which is never required and is not needed
;                        when installing the shim package, can be installed to
;                        make SmartPass change the browser proxy settings
;                        on startup. This functionality used to be in the base
;                        product but now is an optional component.
;            PKI       - Public Key authentication
```

```
;Execute=
; Purpose:   This entry specifies what program to execute after the
;            software has been installed
; Default:   No default
; Example:   Execute=vspstart -h http://www.v-one.com:3845/OLR
;            will cause the On-Line Registration process to be invoked.
; Example:   Execute=card_format /d
;            will cause the smart card formatting utility to be invoked.
;            The following flags can be used with the card_format program
;               /p  -  format card in PCAT reader
;               /s  -  format card in Smarty reater
;               /c  -  format card in CHIPDRIVE extern reader
;               /d  -  format card in current reader if it is a PCAT, Smarty,
;                      or CHIPDRIVE
; Example:   Execute=card_format /d vspstart -h http://www.v-one.com:3845/OLR
;            will cause the smart card formatting utility to be invoked,
;            and on completion of that utility, On-Line Registration to
;            be invoked.
; Notes:     The named program will be invoked at the end of the install
;            process.

;ExecutePrompt=
; Purpose:   This text will appear in a user prompt, asking the user
;            if they want to invoke the program named in 'Execute'
;            after installation or following the next reboot if the
;            installation requires one.
; Default:   No default
; Example:   ExecutePrompt=SmartPass On-Line Registration
; Example:   ExecutePrompt=Smart Card Formatting
; Notes:     If no prompt is specified then the program will be invoked
;            without first prompting the user.

;Remove22x=
; Purpose:   This entry configures the installation program to detect
;            the existence of SmartPass 2.2.x products and remove the
;            programs as part of the installation procedure.
; Default:   No default
; Example:   Remove22x=YES ( not case sensitive )
; Notes:     In case of SmartPass 2.2.x products, any existing VCATs
;            under the program directory will also be deleted.

;WSOCK32WARN1=Warning - A non-standard system component (WSOCK32.DLL) is currently
installed on this machine.
;
;WSOCK32WARN2=Continuing with this installation may cause some installed programs
not to work properly.
;
;WSOCK32WARN3=We recommend that you cancel this installation and contact your
systems administrator.
;
;WSOCK32WARN4=Cancel this installation?
;
;Purpose:     This entry configures the installation program message
;             which will be displayed if the WSOCK32.DLL currently in the
;             windows system directory is from a vendor other than V-ONE
;             or Microsoft.
; Default:    As listed in above commented lines
; Example:    WSOCK32WARN3=We recommend that you cancel this installation
;             and contact the Help Desk at 123-1234.
```

```
;
;PrimaryWINSServer=
; Purpose: This entry configures the installation program to set the Primary
;     Server to the specified IP address
; Default: No default
; Example: PrimaryWINSServer=10.0.0.222
; Notes:  This is only available when the IPSEC package is installed

;SecondaryWINSServer=
; Purpose: This entry configures the installation program to set the Secondary
;     Server to the specified IP address
; Default: No default
; Example: SecondaryWINSServer==10.0.0.223
; Notes:  This is only available when the IPSEC package is installed
;
;DetectCardRemovalInternal=
; Purpose: This entry configures the installation program to set the smart card
; removal detection time interval.
; Default: No default
; Valid Range: 10 - 3600 seconds
; Example: DetectCardRemovalInterval=30
;
;PortList=
; Purpose: This entry configures which ports, in order, that SmartPass will try to
;   navigate through a firewall to initiate a secure session to the SmartGate
;  Server.
;Default: 3845,443,80
;Valid Range: A comma deliminated list of integer values between 1 and 65536
;Example: 3845,443,80,6830
;Warning: Do NOT use port 443 or 80 if either an SSL Server or a Web Server, respectively,
     is running on your SmartGate Server.
```

SmartPass Installation Package Files

Table A–1 lists the SmartPass Installation Package files. The necessity and inclusion of individual files are dependent on which authentication method is being used.

Table A–1, Installation Package Files, Authentication Methods

Installation Package Files	VCAT Token	FIPS Token	PCAT Reader	Smarty Reader	CHIPDRIVE Reader	SecurID	RADIUS	Netrust	Entrust	PKI	Default Files
_inst32i.exe	R	R	R	R	R	R	R	R	R	R	D
_isdel.exe	R	R	R	R	R	R	R	R	R	R	D
_setup.dll	R	R	R	R	R	R	R	R	R	R	D
_setup.lib	R	R	R	R	R	R	R	R	R	R	D
browser.z	O	O	O	O	O	O	O	O	O	O	N
cardfmt.z	U	U	O	O	O	U	U	U	U	U	N
disk1.id**	R	R	R	R	R	R	R	R	R	R	D
entrust.ini**	U	U	U	U	U	U	U	R	R	U	N
install.z	R	R	R	R	R	R	R	R	R	R	D
mcos.z	R	R	O*	O*	U	U	U	U	U	U	D
pcat.z	U	U	R	U	U	U	U	U	U	U	N
readme.txt	R	R	R	R	R	R	R	R	R	R	D
setup.exe	R	R	R	R	R	R	R	R	R	R	D
setup.ini	R	R	R	R	R	R	R	R	R	R	D
setup.ins	R	R	R	R	R	R	R	R	R	R	D
setup.pkg	R	R	R	R	R	R	R	R	R	R	D
shim.z	O	O	O	O	O	O	O	O	O	O	D
spass.z	R	R	R	R	R	R	R	R	R	R	D
starcos.z	U	U	O*	O*	R	U	U	U	U	U	N
tokensys.z	R	R	R	R	R	R	R	R	R	R	D
vcat.z	R	U	U	U	U	U	U	U	U	U	D
chipdrv.z	U	U	U	U	R	U	U	U	U	U	N
fipstokn.z	U	R	U	U	U	U	U	U	U	U	D
ipsec.z	O	O	O	O	O	O	O	O	O	O	N
radius.z	U	U	U	U	U	U	R	U	U	U	N
sgentrus.z	U	U	U	U	U	U	U	U	R	U	N
sgnetrus.z	U	U	U	U	U	U	U	R	U	U	N
sgsdi.z	U	U	U	U	U	R	U	U	U	U	N
smarty.z	U	U	U	R	U	U	U	U	U	U	N
entrust.z**	U	U	U	U	U	U	U	U	R	U	N
netrust.z**	U	U	U	U	U	U	U	R	U	U	N
pki.z	U	U	U	U	U	U	U	U	U	U	N

R This file is required for the functioning of that authentication method
O This file is optional for this functioning of that authentication method
U This file is unnecessary for the functioning of that authentication method and can be deleted
D This file will be included on the installation disk(s) by default
N This file will not be included o n the installation disk(s) by default

*At least one type of smart card must be used, either MCOS, MCOS–B, or STARCOS.

***These files must be obtained from the Entrust or Netrust software and copied onto the installation disk.

Index

A

Access Code 11, 12, 14, 20–21, 93
  change 35–68, 41–68
    SmartPass for UNIX 72
  features 14
ACE/Server 21, 42, 89
AppName 26, 114
authentication key 13
  change 36, 42
Authentication Methods 78
authentication token 12
  CHIPDRIVE extern card reader 37–42
  Entrust 22, 48–53
  FIPS token 19, 88
  FIPS Token (FIPS 140-1) 69, 92–94
  Netrust 22, 53
  PCAT smart card reader 37–42
  PKI 54–59
  preparing 32–53
  RADIUS 21, 45–48, 89, 97–98
  SecurID 21, 42–45, 89, 95–96
  Smarty smart card reader 37–42
  VCAT smart card emulator 33–36, 88, 92–94

B

branding options 26
branding/localizing SmartPass 4.x 26
browser configuration 24

C

CD-ROM 29
CHIPDRIVE extern reader 20, 37–42
  configure as default reader 38–68

D

detecting smart card removal 27
detection/removal of SmartPass 2.x.x 26–27
Dynamic Configuration 11, 12

E

Entrust authentication 22, 48–53
  .epf file 50
  configure SmartPass 51–53
  firewall navigation 52–68
  perform OLR 49–68
Entrust/Netrust
  Authorization code 50
  Reference number 50
ethernets 11
Execute 25, 116
ExecutePrompt 26, 116
exit routines 28

F

files
  detailed descriptions
    setup.ini 113
  setup.ini options 18, 114–123
    AppName 26
    Execute 25–28, 116
    ExecutePrompt 26, 116
    OLRPage 25–28, 114, 115
    Packages 18, 114
    PrimaryWINSServer 118
    Remove22x 26–27, 117
    SecondaryWINSServer 119
    WSOCK32WARNx 118
FIPS Token (FIPS 140-1) 19, 88
  using on a Macintosh 92–94
  using on UNIX SmartPass 69
  using with CE/Pocket PC devices 76
FIPS Token Authentication 78
firewall navigation 59
  Entrust authentication 52
  SecurID authentication 43, 46
  using a Macintosh 99–101
  using UNIX SmartPass 72
format code 20–21, 34–68

FTP
  Proxy 65–68
    use SSL tunneling proxy 65

G

generating random data 31
generic proxy (sgate) 64–68
  use SSL tunneling proxy 64

H

HotJava 73

I

Intel System 14
Internet Control Panel 100
InternetConfig 99
introduction 11–16
IPSec 23–24
  setting WINS Server address 118
  Setting WINS Server Addresses 23–24

M

Macintosh operating systems (Mac OS)
  SmartPass requirements 15
mainframes 11

N

Netrust authentication 22, 53

O

OLRPage 25, 115
On-Line Registration (OLR)
  configuring
    launching options 25–26, 115–117
    SmartPass (Mac) 88
    SmartPass 4.x 25, 25–26
  perform 32
    using Entrust 49–68
  perform on a Macintosh 94
  perform on UNIX SmartPass 71–72
overview 7–8

P

Packages 114
PCAT reader 20, 37–42
  change Access Code 41–68
  change authentication key 42
  configure as default reader 38–68
  format 39–68
PKI authentication 24, 54–59
  adding servers using OLR 56–57
  configure SmartPass 58–61
    PKCS #12 File 59
  firewall navigation 59–68
  logging on 54–56
Pocket PC devices 76. *See also* SmartPass CE/Pocket PC
  hardware requirements 15
PortList 117
  Deployability 117
PrimaryWINSServer 118
proxy
  FTP options 65–68
  generic options 64–68
  SSL options 67–68
  Web options 66–68

R

RADIUS authentication 21, 45–48, 89
  access-challange request 48, 98
  configuring SmartPass 45–68
  launching SmartPass 46–48
    using a Macintosh 97–98
Remove22x 26, 117

S

SecondaryWINSServer 119
SecurID authentication 21, 42–45
  ACE/Server 42
  configuring SmartPass 42–68, 89
  firewall navigation 43–68, 46–68
  launching SmartPass 43–45
    using a Macintosh 95–96
  SmartPass CE/Pocket PC 77, 79–81
Servers
  ACE 42

setup.ini
detailed description 113
detection options 26–27, 27, 117
installation packaging 17–24, 114–115
OLR Launching Options 27
OLR launching options 25–26, 115–117
option descriptions 114–123
shim warnings 118, 118–123
splash screen labeling 26, 114
sgate 64
sgftp 65
Single Port Proxy
change default proxy 103
Single Port Setting 83
smart cards
formatting program 20, 37
physical 11, 13
G&D STARCOS 21, 40–68
Gemplus MCOS 20, 39–68
readers 37–42
CHIPDRIVE 20, 37–42
PCAT 20, 37–42
set up 37–68
Smarty 20, 37–42
virtual 11, 13
FIPS token 19, 88
VCAT token 19, 33–36, 88
SmartGate Server 13
user database 13
SmartGate System
Access Code 14
components 12–14
SmartPass 13
SmartPass
new features 15–16
SmartPass (Macintosh) 87–103
add/change authentication key 103
backing up virtual token 102
changing token's location 102
configuring a proxy 99–101
enabling your token 91
general file locations 101
installing 90
"Macintosh USERS" notes 13
multiple users 101
other system functions 102–103
performing On-Line Registration 94
prepare for distribution 89
prepare On-Line Registration 88
RADIUS Authentication 89, 97–98
running secure applications 98
SecurID Authentication 89, 95–96
Single Port client
changing the default Single Port Proxy 103
uninstalling 102
virtual tokens 88, 92–94
SmartPass 4.x 17–28, 29–68
branding/localizing installation program 26
configure authentication token 32–53
CHIPDRIVE extern reader 37–42
Entrust 48–53
Netrust 53
PCAT smart card reader 37–42
PKI 54–59
RADIUS 45–48
SecurID 42–45
Smarty smart card reader 37–42
VCAT 33–68
configure WINS Server 118–123
detecting smart card removal 27
detection/removal of SmartPass 2.x.x 26–27, 117
Entrust Profiles 50–68
files 113–123
installing 29–31
setting WINS Server address 30–31
launching 31
options display 61–68
perform On-Line Registration 32
using Entrust 49–68
prepare installation package 17–24, 114–115
browser configuration 24
CHIPDRIVE reader 20
Entrust authentication 22
FIPS Token (FIPS 140-1) 19
IPSec 23–24
Netrust authentication 22
PCAT reader 20

PKI 24
RADIUS authentication 21
SecurID authentication 21
smart card formatting program 20–21
Smarty reader 20
VCAT token 19
Winsock function call interception 22–24
prepare On-Line Registration 25–26
OLR launching options 25–26, 115–117
proxy options 63–68
run-time behavior 61–63
setting shim warnings 118
SmartPass deployability option 27
unattended operations feature 28
User Interface
confirmation options 62–68
details view 60
FTP Proxy options 65–68
general options 61–68
Generic Proxy options 64–68
log view 61
logging options 63
server tree list view 60
SSL Proxy options 67–68
toolbar 61
Web Proxy options 66–68
SmartPass CE/Pocket PC 75–86
add/change your authentication key 84
authentication methods
FIPS 76–86
SecurID 77–86
configuring 81–84
installing and launching 78–81
options 82–83
setting up 77
single port setting 83–85
toolbar 86
using 84–86
SmartPass deployability option 27
SmartPass for UNIX 69–74
authentication methods
FIPS token 69
configuring
command line variables 71
OLR commands 72
Web browser 73
installing 70–71
tar command 70
launching 73
performing OLR 71–72
SmartPass software 13
hardware/software requirements 14–15
Smarty reader 20, 37–42
change Access Code 41–68
change authentication key 42
configure as default reader 38–68
format 39–68
spsgftp 65
SSL Proxy 67–68
using a Macintosh 100–101
Sun SPARC System 69
SmartPass for Linux 15
SmartPass for Solaris 15
sweb 66

T

TCP/IP 14
interoperability 11
token rings 11

U

Unattended operations feature 28
UNIX environment
SmartPass requirements 15
UNIX SmartPass 69–74
configuring
command line variables 71
OLR commands 72
Web browser 73
FTP 74
installing 70–71
launching 73
performing OLR 71–72
Telnet 74
user database (sguserdb) 13
Using SmartPass CE/Pocket PC 84

V

VCAT smart card emulator 19, 88
  add/change authentication key 36
  change Access Code 35–68
  configure as default reader 33–68
  format 34–68
  using on a Macintosh 92–94

W

Web Proxy (sweb) 66–68
  using a Macintosh 99–100
Windows CE devices 76
  hardware requirements 15
Windows environment 11
  SmartPass requirements 14
  taskbar tray 60
Windows NT System
  SmartPass requirements 14
  SmartPass w/dialup 30–31
WINS Server address 30–31
Winsock function call interception 22–24
wsock.z 22–24
wsock32.dll 22–24
WSOCK32WARNx 118
wsockx.dll 22